THE ELECTRICITY SECTOR'S EFFORTS TO RESPOND TO CYBERSECURITY THREATS

HEARING

BEFORE THE

SUBCOMMITTEE ON ENERGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

FEBRUARY 1, 2017

Serial No. 115–3

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

24–845 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 ENERGY AND COMMERCE

GREG WALDEN, Oregon
Chairman

JOE BARTON, Texas
Vice Chairman
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
TIM WALBERG, Michigan
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
EARL L. "BUDDY" CARTER, Georgia

FRANK PALLONE, JR., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CARDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan

SUBCOMMITTEE ON ENERGY

FRED UPTON, Michigan
Chairman

PETE OLSON, Texas
Vice Chairman
JOE BARTON, Texas
JOHN SHIMKUS, Illinois
TIM MURPHY, Pennsylvania
ROBERT E. LATTA, Ohio
GREGG HARPER, Mississippi
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
KEVIN CRAMER, North Dakota
TIM WALBERG, Michigan
GREG WALDEN, Oregon *(ex officio)*

BOBBY L. RUSH, Illinois
Ranking Member
JERRY MCNERNEY, California
SCOTT H. PETERS, California
GENE GREEN, Texas
MICHAEL F. DOYLE, Pennsylvania
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont
PAUL TONKO, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
G.K. BUTTERFIELD, North Carolina
FRANK PALLONE, JR., New Jersey *(ex officio)*

CONTENTS

THE ELECTRICITY SECTOR'S EFFORTS TO RESPOND TO CYBERSECURITY THREATS

WEDNESDAY, FEBRUARY 1, 2017

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ENERGY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:15 a.m., in room 2322 Rayburn House Office Building, Hon. Fred Upton (chairman of the subcommittee) presiding.

Present: Representatives Upton, Olson, Barton, Shimkus, Murphy, Latta, Harper, McKinley, Johnson, Long, Flores, Mullin, Hudson, Cramer, Walberg, Walden (ex officio), Rush, McNerney, Peters, Doyle, Castor, Sarbanes, Welch, Tonko, Loebsack, Schrader, Kennedy, Butterfield, and Pallone (ex officio).

Staff present: Will Batson, Legislative Clerk, E&P; Ray Baum, Staff Director; Jordan Davis, Director of Policy and External Affairs; Wyatt Ellertson, Research Associate, Energy/Environment; Adam Fromm, Director of Outreach and Coalitions; Tom Hassenboehler, Chief Counsel, Energy/Environment; Zach Hunter, Director of Communications; A.T. Johnston, Senior Policy Advisor/Professional Staff, Energy/Environment; Katie McKeough, Press Assistant; Brandon Mooney, Senior Policy Advisor, Energy; Mark Ratner, Policy Coordinator; Annelise Rickert, Counsel, Energy; Dan Schneider, Press Secretary; Peter Spencer, Professional Staff Member, Energy; Evan Viau, Staff Assistant; Jeff Carroll, Minority Staff Director; David Cwiertny, Minority Energy/Environment Fellow; Rick Kessler, Minority Senior Advisor and Staff Director, Energy; John Marshall, Minority Policy Coordinator; Alexander Ratner, Minority Policy Analyst; Andrew Souvall, Minority Director of Communications, Outreach and Member Services; Tuley Wright, Minority Energy and Environment Policy Advisor; and C.J. Young, Minority Press Secretary.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. The Subcommittee on Energy will now come to order. Apologize for the delay. There were some technical difficulties with the cameras but they are now working. So everybody looks good and in color.

I recognize myself for 5 minutes. Today's hearing is going to examine what the electricity sector is currently doing to prepare for and respond to cybersecurity threats to the nation's electricity transmission systems.

News reports bombard us almost daily about malware infections and portrayals of the harm from cyber-attacks. We've read alarming descriptions of what might happen if there is successful widespread attack on the critical infrastructure of the electricity system and the potential challenges to recovering from such an attack.

It is unquestionable that ensuring the reliable supply of electricity is absolutely vital to our nation's security, economy, our health and welfare.

In Michigan and across the country, electricity enables telecommunications, financial transactions, the transport and delivery of energy, food, everything. It powers the infrastructure that delivers our drinking water. It enables businesses and industry to make and provide the goods and services of our modern society and it powers our hospitals and our households.

So cyber threats to reliability deserve our constant examination. But as we do so, we have to recognize that ensuring reliability is the central function of electricity grid operations, and a tremendously complex system has developed over time to ensure that the lights stay on. Given the unique nature of electricity, the system operates to address the occasional loss of transmission components and to avoid cascading failures. It doesn't always succeed, but large-scale blackouts have been rare for a reason.

Nevertheless, new risks are emerging rapidly. The integration into the system of new technologies, especially digital technologies, that are essential for keeping up with the nation's energy needs constantly adds new vulnerabilities. Combine this with the rapid development of cyber-attacks and safeguarding transmission infrastructure becomes particularly challenging.

In recent years, Congress has enhanced the ability of the electricity sector to address emerging cyber and physical threats. In the last Congress, this committee wrote provisions included in the FAST Act that sought to facilitate sharing of threat information between the private sector asset owners and the federal government. Other measures enhanced authorities for taking emergency action against cyber and physical attacks.

At the same time, the NERC, operating through authorities authored by this committee, has been establishing and enforcing critical infrastructure protection standards and coordinating a number of other activities to confront these threats. Industry and federal authorities have been working to address those risks.

We have taken testimony that outlines these activities in recent years, and I think that evidence shows that utilities and transmission operators are not sitting still.

I don't think that anyone will dispute that improvements in operational practices, information sharing, defensive planning, supply chain controls, hardening of infrastructure remains necessary. And nobody will dispute that someday, an attack may succeed in taking down these components. So how does the industry plan to respond?

This hearing will update the subcommittee on the state of the various NERC and industry activities to mitigate risks and respond to cyber-attacks. This will inform two objectives.

First, this subcommittee's agenda for the Congress will include a close focus on the various structural, economic, and technological factors that are affecting development of the nation's electricity

systems. We'll be examining policies that may need to be reformed to ensure this system adequately meets the demand of consumers in coming decades, and a key aspect of any of this work will certainly involve enhancing reliability in the evolving electricity system to meet the demands of the digital age.

And second, we must continue to build a record about electric sector efforts to address cyber security threats. This will help us identify whether additional measures are necessary. In time, we will hear from DOE, FERC and other agencies, but developing a clear picture today about what the industry actually is doing will be critical to this ongoing effort.

With that as a backdrop, let me welcome our witnesses. Our panel today provides a number of important perspectives. We will hear from NERC, the industry's reliability organization responsible for setting and enforcing standards. We will hear how the industry coordinates cybersecurity planning and response. We will hear perspective from a critical infrastructure expert, and we'll hear from someone responsible for cybersecurity in the actual operations of transmission systems.

This panel this morning should help cover a range of topics from security standards to information sharing, recovery planning. It's going to help us understand where gaps may be going forward, and we welcome that testimony.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON

Today's hearing will examine what the electricity sector is currently doing to prepare for and respond to cybersecurity threats to the nation's electricity transmission systems.

News reports bombard us almost daily about malware infections and portrayals of the harm from cyber attacks. We've read alarming descriptions of what might happen if there is successful, widespread attack on the critical infrastructure of the electricity system-and the potential challenges to recovering from such an attack.

It is unquestionable that ensuring the reliable supply of electricity is absolutely vital to our nation's security, economy, our health and welfare.

In my home state of Michigan and across the country, electricity enables telecommunications, financial transactions, the transport and delivery of energy, food. It powers the infrastructure that delivers our drinking water. It enables business and industry to make and provide the goods and services of our modern society. It powers our hospitals, our households.

So cyber threats to reliability deserve our constant examination. But as we do so, we should also recognize that ensuring reliability is the central function of electricity grid operations-and a tremendously complex system has developed over time to ensure our lights stay on. Given the unique nature of electricity, the system operates to address the occasional loss of transmission components and to avoid cascading failures; it doesn't always succeed, but large scale blackouts have been rare for a reason.

Nevertheless, new risks are emerging rapidly. The integration into the system of new technologies-especially digital technologies-that are essential for keeping up with our nation's energy needs constantly add new vulnerabilities. Combine this with the rapid development of cyber threats and safeguarding transmission infrastructure becomes particularly challenging.

In recent years, Congress has enhanced the ability of the electricity sector to address emerging cyber and physical threats. In the last Congress, this Committee wrote provisions included in the FAST Act that sought to facilitate sharing of threat information between private sector asset owners and the federal government. Other measures enhanced authorities for taking emergency action against cyber and physical attacks.

At the same time, the North American Electric Reliability Corporation (NERC)—operating through authorities authored by this Committee-has been establishing

and enforcing critical infrastructure protection standards and coordinating a number of other activities to confront these threats. Industry and federal authorities have also been working to address risks.

We've taken testimony that outlines these activities in recent years. And I think the evidence shows that utilities and transmission operators are not sitting still.

But I don't believe anybody will dispute that improvements in operational practices, information sharing, defensive planning, supply chain controls, hardening of infrastructure remain necessary. And nobody will dispute that someday, an attack may succeed in taking down critical components; how does the industry plan to respond to that?

Today's hearing will update the subcommittee on the state of the various NERC and industry activities to mitigate risks and respond to cyber attacks. This will inform two objectives:

First, the energy subcommittee's agenda for this Congress will include a close focus on the various structural, economic, and technological factors that are affecting development of the nation's electricity system.

We'll be examining policies that may need to be reformed to ensure this system adequately meets the demands of consumers in coming decades. And a key aspect of any of this work will involve enhancing reliability in the evolving electricity system to meet the demands of the digital age.

And second: we must continue to build a record about electric sector efforts to address cyber security threats. This will help the subcommittee identify whether additional measures, are necessary. In time, we will hear from DOE, FERC and other agencies, but developing a clear picture today about what the industry actually is doing will be critical to this ongoing effort.

With that as a backdrop, let me welcome our witnesses. Our panel today provides a number of important perspectives: We'll hear from NERC, the industry's reliability organization responsible for setting and enforcing standards; we'll hear how the industry coordinates cybersecurity planning and response; we'll hear perspective from a critical infrastructure expert; and we'll hear from somebody responsible for cybersecurity in the actual operations of transmission systems.

The panel this morning should help cover a range of topics-from security standards to information sharing and recovery planning. It should help us discuss the various levels of cyber and related physical risks to electricity infrastructure and how they are addressed. And it should help us understand where gaps may be going forward.

Mr. UPTON. At this point, I recognize the ranking member of the subcommittee, my friend from Chicago, Mr. Rush.

OPENING STATEMENT OF HON. BOBBY L. RUSH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. RUSH. I want to thank you, Mr. Chairman, for this opportunity and for this hearing.

Mr. Chairman, this is an important hearing on the electricity sector's efforts to respond to cybersecurity threats. Mr. Chairman, this is a very first step in examining the critical issue of a electricity sector cybersecurity.

I look forward, Mr. Chairman, to engaging our distinguished panel of industry witnesses and their recommendations designed to protect the grid from external threats.

However, Mr. Chairman, I am sure we will all agree that additional information is needed to truly appreciate the expanding host of challenges that could potentially threaten the U.S. electrical sector.

Mr. Chairman, it is my understanding that you have committed to holding at least one additional hearing with agency stakeholders in the near future so that the members of this subcommittee will have a greater and a fuller appreciation for the security issues facing the grid.

The issue of external forces hacking into most public and private domestic targets is one that is front and center on the minds of most of the American people.

If recent history is any indication, then it's not a matter of if, Mr. Chairman, but, rather, when some threat, whether it be a national disturbance, an individual hacker, a rogue state or even a well-known foreign power challenges the resiliency of our nation's energy infrastructure.

Mr. Chairman, we are all aware the cyber-attack in the Ukraine this past December that left over 225,000 people without power in Kiev as a result of suspected Russian hacking.

While we have been fortunate, Mr. Chairman, to date in that we haven't suffered any major cybersecurity attacks on our own grid, let us not become complacent and wait until an event occurs.

Many of us, Mr. Chairman, still view Russia, among other countries, as a potential threat to the U.S. grid system and we cannot risk our safety and security on the whims of Putin or any other foreign leader who may try to do us harm.

Quite the contrary, we must be prudent and proactive in securing our electrical grid and part of that strategy must include close cooperation and collaboration between the public and private sectors.

As was noted, in the last quadrennial energy review conducted by the Obama administration in January 2014, there is still work to do to improve the information sharing processes between government and industry.

Additionally, we must ensure that our grid is protected from some of the specific challenges of today's world. We must make certain that the electricity sector is secure, even in the place of an aging infrastructure and a changing energy portfolio.

That would include more distributed energy, smart grid technologies and other advanced technologies. Mr. Chairman, it is vital that Congress examines the state of the grid and provides real leadership in regards to modernizing our grid and making sure that it's secure for the challenges of the 21st century.

With that, I yield back.

Mr. UPTON. Thank you. I understand that Chairman Walden is on his way but he's not quite here. So we will go to Ranking Member Pallone for an opening statement.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Mr. Chairman. Greg was at the other hearing.

I want to thank you for holding today's hearing evaluating the cybersecurity threats to the electricity sector in our country and, of course, I welcome you to this new role as chairman of the Energy Subcommittee.

You and I accomplished a great deal together in the last Congress and I hope to work together with you, Mr. Rush, on critical energy policy in this Congress.

This hearing is a good first step for our committee to look into the impacts of cybersecurity threats on the electricity grid.

However, I believe that we need more hearings and a deeper analysis of the issue so members can truly understand the challenges and threats facing our grid and I appreciate the chairman's willingness to honor Ranking Member Rush's request to hold another hearing on this topic with federal government witnesses, especially from the Department Energy and the Federal Energy Regulatory Commission.

Their perspective and experience on this issue will be vital to the committee's oversight efforts and I also believe that the committee should hold a closed-door hearing to look at the cybersecurity risk to our electricity grid.

There are classified aspects of this issue that can't be discussed in a public hearing like this and members deserve the opportunity to be briefed on this high-level information in order to ensure we are adequately protecting the grid from threats.

To date, the industry has done a commendable job of guarding electricity consumers against losses caused by cyber-attack. But make no mistake, the threats are out there.

In December 2015, Russian state hackers successfully compromised the Ukraine's electric grid, shutting down multiple distribution centers and leaving more than 200,000 residents without power for their lights and heaters.

That attack was premeditated and well-choreographed with groundwork that predated the full attack by many months. It was sophisticated and synchronized, taking down backup power supplies and jamming phone lines to keep operators unaware of the extent of damages. And to date, it stands as the only recognized cyber-attack to successfully take down a power grid.

Certainly, there are vast differences between the system in the Ukraine and our own grid. So it's tempting to dismiss events in the Ukraine as something that could never happen here.

But we owe it to the American people to ask whether anything about that attack could be replicated here, what lessons can we learn to make our electric grid more secure and utility workers more vigilant of cybersecurity threats.

And what should be the priorities of this committee and this Congress to ensure that a successful cyber-attack on the electric grid never happens on American soil? If Russia hacked our election, what's to stop them from hacking our electricity grid?

Now, our committee has not been idle when it comes to grid security. Last Congress, Chairman Upton, with my support and the support of many members of the committee, pushed through legislation to enhance the security of our group from cyber and other threats.

I was pleased to see that signed into law by President Obama because I consider grid security to be a top tier national security concern.

And yet, just days ago President Trump signed a presidential memorandum establishing the members of the National Security Council's principles committee and it appears that the Secretary of Energy, who Congress just made the lead federal official responsible for securing our electricity grid, has been booted off this significant interagency advisory panel, and this is incredibly troubling

and I strongly urge the president to reconsider his decision to sideline DOE from the national security dialog.

I would hope that my Republican colleagues would join me in asking the president to reverse this decision. It's inexcusable, in my opinion, that there no longer appears to be room at the top level of the National Security Council for the secretary of energy who also is in charge of nuclear security but there is a permanent slot for Steve Bannon, his chief strategist.

Essentially, President Trump has chosen his top political security advisor over the nation's top energy security advisor and that's a recipe for disaster.

I hope my colleagues will join me in conveying that view to the White House before something happens that endangers our economy and our people because the safety of our grid and our nuclear arsenal are too important.

I don't know if anybody else wants my time. Otherwise, I'll yield back.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Mr. Chairman, thank you for holding today's hearing evaluating the cybersecurity threats to the electricity sector in our country. I welcome you to this new role as Chairman of the Energy Subcommittee. You and I accomplished a great deal together in the last Congress, and I hope to work together with you and Mr. Rush on critical energy policy in this Congress.

This hearing is a good first step for our committee to look into the impacts of cybersecurity threats on the electricity grid. However, I believe that we need more hearings and a deeper analysis of the issue so members can truly understand the challenges and threats facing our grid. I appreciate the Chairman's willingness to honor Ranking Member Rush's request to hold another hearing on this topic with federal government witnesses, especially from the Department of Energy and the Federal Energy Regulatory Commission. Their perspective and experience on this issue will be vital to the Committee's oversight efforts. I also believe that the Committee should hold a closed-door hearing to look at the cybersecurity risks to our electricity grid. There are classified aspects of this issue that cannot be discussed in a public hearing like this, and Members deserve the opportunity to be briefed on this high-level information in order to ensure we are adequately protecting the grid from threats.

To date, the industry has done a commendable job of guarding electricity consumers against losses caused by a cyberattack. But make no mistake: the threats are out there.

In December 2015, Russian state hackers successfully compromised the Ukraine's electric grid, shutting down multiple distribution centers and leaving more than 200,000 residents without power for their lights and heaters. That attack was premeditated and well-choreographed, with groundwork that pre-dated the full attack by many months. It was sophisticated and synchronized, taking down backup power supplies and jamming phone lines to keep operators unaware of the extent of damages. To date, it stands as the only recognized cyberattack to successfully take down a power grid.

Certainly, there are vast differences between the system in the Ukraine and our own grid, so it's tempting to dismiss events in the Ukraine as something that could never happen here. But we owe it to the American people to ask whether anything about that attack could be replicated here. What lessons can we learn to make our electric grid more secure and utility workers more vigilant of cybersecurity threats? And, what should be the priorities of this Committee and this Congress to ensure that a successful cyberattack on the electric grid never happens on American soil? If Russia hacked our election, what's to stop them from hacking our electricity grid?

Now, our Committee has not been idle when it comes to grid security. Last Congress, Chairman Upton, with my support and the support of many members of the Committee, pushed through legislation to enhance the security of our grid from cyber and other threats. I was pleased to see that signed into law by President Obama because I consider grid security to be a top tier national security concern.

And yet, just days ago, President Trump signed a presidential memorandum establishing the members of the National Security Council's Principals Committee—and it appears the Secretary of Energy—who Congress just made the lead federal official responsible for securing our electricity grid—has been booted off this significant interagency advisory panel.

This is incredibly troubling and I strongly urge the President to reconsider his decision to sideline DOE from the national security dialogue. I would hope that my Republican colleagues would join me in asking the President to reverse this decision. It is inexcusable that there no longer appears to be room at the top level of the National Security Council for the Secretary of Energy—who also is in charge of nuclear security—but there is a permanent slot for Steve Bannon, his chief strategist. Essentially, President Trump has chosen his top political security advisor over the nation's top energy security advisor—and that's a recipe for disaster. I hope my colleagues will join me in conveying that view to the White House before something happens that endangers our economy and our people. The safety of our grid and our nuclear arsenal are too important.

I yield back.

Mr. UPTON. The gentleman yields back.

I just want to tell the gentleman that we do anticipate having some classified hearings as to cyber. So I know everyone has signed a pledge, so look forward to having that happen.

At this point, I'll yield 5 minutes to the full committee chairman, my friend, the gentleman from Oregon, Mr. Walden.

Mr. WALDEN. Thank you, Mr. Upton.

Mr. UPTON. Welcome to your first appearance before the subcommittee as full committee chair.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. I am delighted to be here, and I am delighted you're chairing this subcommittee. I wish you could have been downstairs for the beginning of the Health Subcommittee because we had a nice big University of Oregon "O" come up on the new screen there to match your green hearing room.

Good morning, and I am pleased that the ranking member has such strong confidence in the new Secretary of Energy. We think he's a good man, too, and look forward to working with him on this committee.

One of the humbling responsibilities for members of the Energy and Commerce Committee is to fully appreciate the power we have to make policy changes that can have enormous and positive impacts on American consumers for decades to come.

From health care, to manufacturing and trade, to telecommunications, transportation, and the delivery of energy, our goal is to identify how to position the United States to be able to harness the tremendous potential of digital communications for all sectors of the economy, while minimizing unintended side effects.

We are witnessing the transformation of American commerce as advances in digital and information technology affect almost everything that we do in our daily lives. And we see how layering new digital ways of doing things onto existing practices and infrastructures creates new risks and potential harm.

Who among us is not frequently seeking out a plug-in so we can keep our various electronic devices charged? We are really tethered.

Never has the reliability of the electric grid been more important to everything in our lives. That also means never has the electric

grid been more of a potential target for disruption by nefarious actors.

The hearing today concerns what is being done to address and respond to the cybersecurity threats to our nation's electricity system.

By any measure, the reliable supply of electricity is an essential part of almost everything that we do, and its loss—even for short periods of time—can have expensive and life-threatening consequences.

Unfortunately, cyber threats in this sector are unavoidable, and they are growing. This is due to the dynamic nature of the information flows in the modern world as well as the increasing sophistication of hackers and adversaries.

Threats in these flows will only grow as the instant information and communications enabled by digital technology become more essential for our electricity system to operate at increased levels of reliability.

Looking forward, it's clear the growth of digital technology will constantly introduce new avenues for cybersecurity threats. They must be managed effectively.

Responsibility for addressing these threats, while harnessing the promise of digital technology, rests largely on the thousands of people involved in planning and operating our nation's complex electricity transmission systems, as well as the organizations charged with ensuring reliability.

This morning we will hear from industry and cybersecurity experts who can provide us a report on the state of cybersecurity planning and practices.

Our witnesses will help us understand just what is being done to address cybersecurity threats and how the industry plans to confront new threats as they emerge. The hearing will help us begin to understand more fully where the electricity sector is and where it should be in terms of cybersecurity and related risk to electric reliability.

This will lay the groundwork for closer scrutiny of the relevant policies necessary to ensure future reliability in an evolving electricity, and, frankly, digital sectors.

There are many questions to pursue, such as, how is cybersecurity planning being embedded in procurement and other systems planning by the industry? What measures are being implemented to prepare for successful attacks, so that—just as with nature's constant threats—if the lights do go out, can we get them back on quickly?

And I know all of you run that grid test periodically and the tabletopping of it. So we will be interested to hear more about that.

What's being developed to address the truly high consequence of the low probability events that can have the most devastating impacts? And what more can be done?

We really appreciate your testimony. I've read through it and we are enhanced by your counsel. We look forward to working with you.

With that, Mr. Chairman, I yield back the balance of my time.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

One of the humbling responsibilities for members of the Energy and Commerce Committee is to fully appreciate the power we have to make policy changes that can have enormous and positive impacts on American consumers for decades to come. From health care, to manufacturing and trade, to telecommunications, transportation, and the delivery of energy, our goal is to identify how to position the United States to harness the tremendous potential of digital communications for all sectors of the economy, while minimizing unintended side effects.

We are witnessing the transformation of American commerce as advances in digital and information technology affect almost everything that we do in our daily lives. And we see how layering new digital ways of doing things onto existing practices and infrastructures creates new risks and potential harm. Who among us is not frequently seeking out a plug in so that we can keep our various electronic devices charged? Never has the reliability of the electric grid been more important to everything in our lives. That also means never has the electric grid been more of a potential target for disruption by nefarious actors. The hearing today concerns what is being done to address and respond to the cybersecurity threats to our nation's electricity system.

By any measure, the reliable supply of electricity is an essential part of almost everything we do, and its loss-even for short periods-can have expensive and life threatening consequences. Unfortunately, cyber threats in this sector are unavoidable and growing.

This is due to the dynamic nature of the information flows in the modern world as well as the increasing sophistication of hackers and adversaries. Threats in these flows will only grow as the instant information and communications enabled by digital technology become more essential for our electricity system to operate at increased levels of reliability.

Looking forward, it is clear the growth of digital technology will constantly introduce new avenues for cybersecurity threats that must be managed effectively. Responsibility for addressing these threats, while harnessing the promise of digital technology, rests largely on the thousands of people involved in planning and operating our nation's complex electricity transmission systems, as well as the organizations charged with ensuring reliability.

This morning we will hear from industry and cybersecurity experts who can provide us a report on the state of cybersecurity planning and practices. Our witnesses will help us understand just what is being done to address cybersecurity threats, and how the industry plans to confront new threats as they emerge.

The hearing will help us begin to understand more fully where the electricity sector is and where it should be in terms of cybersecurity and related risks to electric reliability. This will lay the groundwork for closer scrutiny of the relevant policies necessary to ensure future reliability in an evolving electricity sector.

There are many questions to pursue: How is cybersecurity planning being embedded in procurement and other systems planning by the industry? What measures are being implemented to prepare for successful attacks, so that—just as with nature's constant threats-if the lights do go out, can we get them on quickly? What is being developed to address the truly high consequence but low probability events that can have the most devastating impacts? And what more can be done?

As the committee implements its own energy policy agenda, the testimony we take will inform how we approach the future and how we best use innovation and technology to protect American consumers.

Mr. UPTON. Thank you. The gentleman yields back. We are ready for our witnesses.

We are joined by Gerry Cauley, President and CEO of the North American Electrical Reliability Corporation, NERC; Scott Aaronson, Executive Director for the Security and Business Continuity from EEI, Edison Electric, on behalf of the Electricity Subsector Coordinating Council; Barbara Sugg, Vice President for IT and Chief Security Officer of Southwest Power Pool on behalf of ISO/RTO Council; and Dr. Chris Beck, Chief Scientist and Vice President for policy from the Electric Infrastructure Council.

I welcome you all. We appreciate you submitting your testimony early, so we are able to take it home on the last day or two. We

ask you to summarize it and take about 5 minutes in your presentation, at which time we will go to questions.

Mr. Rush, yes.

Mr. RUSH. Mr. Chairman, by way of announcements, we have a former member here, Mike Ross from Arkansas.

Mr. UPTON. It is good to see your face, Mike. Welcome back. A good friend to all of us that served with you. Thank you. Thanks, Bobby.

(Applause.)

Mr. Cauley, you're recognized for 5 minutes.

STATEMENTS OF GERRY W. CAULEY, PRESIDENT AND CEO, NORTH AMERICAN RELIABILITY CORPORATION (NERC); SCOTT I. AARONSON, EXECUTIVE DIRECTOR, SECURITY AND BUSINESS CONTINUITY, EDISON ELECTRIC INSTITUTE (EEI), ON BEHALF OF ELECTRICITY SUBSECTOR COORDINATING COUNCIL; CHRIS BECK, CHIEF SCIENTIST AND VICE PRESIDENT FOR POLICY, THE ELECTRIC INFRASTRUCTURE SECURITY COUNCIL (EIS COUNCIL); BARBARA SUGG, VICE PRESIDENT FOR IT AND CHIEF SECURITY OFFICER, SOUTHWEST POWER POOL (SPP), ON BEHALF OF ISO/RTO COUNCIL (IRC)

STATEMENT OF GERRY W. CAULEY

Mr. CAULEY. Good morning, Chairman Upton, Ranking Member Rush, Committee Chairman Walden, Ranking Member Pallone, and members of the subcommittee.

Thank you for conducting this timely hearing this morning to assess the cybersecurity of the nation's power grid.

The threat of cyber-attack by nation states, terrorist groups and criminals is at an all-time high. In December, as has been mentioned, of 2015, a cyber-attack in the Ukraine left over 225,000 customers without power for several hours.

This indicates that nation state adversaries have the cyber tools and now the will to disrupt the grid of other nations.

More recently, in the U.S., although no effects were seen on the power grid, we saw a million electronic devices all part of the internet of things captured and used in a sudden denial of service attack against internet service providers.

We've seen an increased presence of ransomware, data theft, and other criminal activities against all sectors of our economy. As defined by Congress, NERC's role is to assure the reliability and security of the bulk power system through mandatory standards, enforcement, and through reliability assessments.

Our independent board and staff are not affiliated with the power system owners and operators. FERC approves NERC's standards and enforcement actions in the U.S. and has the authority to direct NERC to produce new standards or to revise existing standards.

As a nation, we share a grid with our fellow countries to the north and south, which is why NERC is an international organization spanning the U.S., Canada and, of course, Mexico.

Our cybersecurity standards, which are developed with the expertise of industry participating in that, provide a strong foundation for security practices across the industry.

As just a few examples, our standards require inventory of cyber assets and configuration management, security perimeters and physical access controls, effective passwords and authentication, the use of certified software and patches, background checks and training of personnel, incident reporting and recovery plans.

NERC, along with our eight regional entities, has cyber experts that conduct hundreds of visits each year to assess cybersecurity controls at these companies.

We are finding that power companies take cybersecurity very seriously with strong attention at the top from CEOs and from boards.

Cyber assets used to operate the grid are separate and isolated from business systems and corporate systems, and also from the public internet. Utility personnel are screened and well trained.

There is a strong culture of security across each company. Companies are using advanced third party services to identify vulnerabilities and threats, and to maintain their system's secure.

Most importantly, power companies know they must continually monitor and detect suspicious activity, isolate malware, and destroy it before anything happens. And this process is commonly known as the kill chain.

As flexible and risk-based as our standards are, I firmly believe that we cannot win a cyber war with regulations and standards alone. Industry must be agile and continuously adapt to threats, and to do that we need robust sharing of information regarding threats and vulnerabilities.

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

One of our most effective tools in this process is the Cybersecurity Risk Information Sharing Program, otherwise known as CRISP. Developed by the Department of Energy, CRISP has been adopted by NERC and deployed across wide areas of the U.S. grid to continuously monitor and detect malicious activity.

Working with the U.S. government analysts at the classified level, we are able to detect problems early and get this information out to industry for action.

When time is of the essence, NERC can also issue alerts to industry at three levels of urgency. The two highest levels of urgency require response from industry back to NERC.

In addition to operating the E–ISAC, NERC conducts an annual security conference, training events and frequent classified briefings. As has been mentioned, we also conduct continent-wide cyber and physical security exercise called GridEx.

Over 4,000 participants from industry and government organizations across North America engage for two days in a very severe massive cyber and physical attack on our grid. The exercise includes a tabletop which industry CEOs and senior government officials coordinate a national response including communications, deployment of resources, cyber mutual assistance, and other strategies.

To date, there has not been a single cyber-attack in North America that has resulted in a power outage to a customer. This is an

exceptional record. However, we will never be complacent. We understand the risk is real. We have hard work to do every day and we will continue to do that.

I thank the Committee for the time today and look forward to your questions. Thank you.

[The statement of Mr. Cauley follows:]

Testimony of Gerry W. Cauley, President and Chief Executive Officer

North American Electric Reliability Corporation

Before the Subcommittee on Energy of the House Energy and Commerce Committee

"The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

February 1, 2017

Good morning Chairman Upton, Ranking Member Rush, members of the subcommittee and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). I am pleased to speak with you today about the responsibilities that Congress has vested in NERC to assure the reliability and security of the bulk power system (BPS) in North America. Given the topic of today's hearing, my testimony focuses on NERC's role in addressing cyber security threats.

The North American BPS is among the nation's most critical infrastructures. Virtually every critical sector depends upon electricity. The BPS is also one of the largest, most complex systems ever created. It is robust and highly reliable. Nevertheless, conventional and non-conventional factors do present risks to the BPS.

Summary

The security landscape is dynamic, requiring constant vigilance and agility. NERC addresses cyber risk through a variety of regulatory and non-regulatory means. Today's testimony will focus on those efforts currently underway by NERC to address cyber security and protect the grid. NERC's mandatory critical infrastructure protection standards (CIP standards) are a foundation for

security practices. They provide universal, baseline protections. Due to the ever-evolving nature of cyber threats, security cannot be achieved through standards alone. Vigilance also requires the agility to respond to new and rapidly changing events. Accordingly, NERC's Electricity Information Sharing and Analysis Center (E-ISAC) serves as the information sharing conduit between the electricity industry and government for cyber and physical security threats. The E-ISAC facilitates communication of important or actionable information, and strives to maintain "ground truth" during rapidly evolving security events. Together, mandatory standards, coupled with effective mechanisms to share information, provide robust and agile tools to protect the BPS. NERC works closely with the Electricity Subsector Coordinating Council (ESCC) to further the public private partnership so important to addressing security.

About NERC

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

NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC performs a critical role in real-time situational awareness and

information sharing to protect the electricity industry's critical infrastructure against threats to the BPS. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. Our jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

Critical Infrastructure Protection Standards

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Electricity Information Sharing and Analysis Center

NERC's CIP standards provide a foundation for security practices. They provide universal, baseline protections. But security cannot be achieved through these standards alone. Because of the emerging and dynamic nature of malicious cyber threats, reliability assurance also requires constant situational awareness, real time communication, and prompt emergency response capabilities. NERC operates the E-ISAC which is a key component in providing these capabilities for the electric sector.

The E-ISAC, in collaboration with the Department of Energy (DOE) and the ESCC, serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

The E-ISAC:[2]

- Identifies, prioritizes, and coordinates the protection of critical power services, infrastructure service, and key resources;
- Facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and practices;
- Provides rapid response through the ability to effectively contact and coordinate with asset owners and operators, as required;
- Authors alerts to industry ranging from advisory notices to essential actions requiring recipients to respond as defined in the alert;
- Provides and shares analysis, which includes capturing and correlating trend data for historical analysis, and sharing that information within the sector;
- Receives incident data from private and public entities;
- Assists DOE, FERC, and the Department of Homeland Security (DHS) in analyzing event data to determine threats, vulnerabilities, trends and impacts for the sector, as well as interdependencies with other critical infrastructures (this includes integration with the DHS National Cybersecurity and Communications Integration Center (NCCIC));

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

- Analyzes incident data and prepares reports based on subject matter expertise in security and the BPS;
- Shares threat alerts, warnings, advisories, notices, and vulnerability assessments with the industry;
- Works with other ISACs to share information and provide assistance during actual or potential sector disruptions whether caused by intentional, accidental, or natural events;
- Develops and maintains an awareness of private and governmental infrastructure interdependencies;
- Provides an electronic, secure capability for the E-ISAC participants to exchange and share information on all threats to defend critical infrastructure;
- Participates in government critical infrastructure exercises; and
- Conducts outreach to educate and inform the electricity sector.

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

NERC Alerts

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

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

NERC determines the appropriate alert notification based on risk to the BPS. Generally, NERC distributes alerts broadly to users, owners, and operators of the North American BPS using its Compliance Registry. Entities registered with NERC are required to provide and maintain updated compliance and cyber security contacts. NERC also distributes the alerts beyond BPS users, owners, and operators to include other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g., Balancing Authorities, Transmission Operators, Generation Owners, etc.).

Alerts are developed with the strong partnership of federal technical organizations, including FERC, DOE National Laboratories, DHS, and BPS subject matter experts. Since 2009, NERC has

issued 41 cyber-related alerts (37 Industry Advisories and 4 Recommendations to Industry). Those alerts covered items such as Sabotage events, Aurora, Stuxnet, Night Dragon, and the reporting of suspicious activity. In 2016, NERC issued two Level Two alerts – the first related to the cyber security event in Ukraine and another concerning distributed denial of service attacks involving compromised Internet of Things[3] devices. Responses to alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders.

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

GridEx

Consistent with our mission to promote a strong learning environment, NERC hosts a biennial grid security exercise – GridEx – which simulates widespread, coordinated cyber and physical attacks on critical electric infrastructure. Led by the E-ISAC, NERC conducted GridEx III on November 18–19, 2015.[4] GridEx III was the largest geographically distributed grid security exercise to date. GridEx III consisted of a two-day distributed play exercise and a separate

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

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

executive tabletop session featuring 32 industry executives and senior officials from federal and state governments. All told, more than 4,400 individuals from 364 industry, law enforcement and government organizations across North America participated in GridEx III.

The objectives of GridEx III were to:

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

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

GridSecCon

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

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

Ukraine

Cyber attacks on three distribution utilities in Ukraine on December 23, 2015, garnered significant attention. The Ukrainian incidents affected up to 225,000 customers in three distribution-level service territories and lasted for several hours.[5] A team from the United States, which included experts from the Department of Energy (DOE), the Department of Homeland Security (DHS), the Federal Bureau of Investigation and NERC, assisted the government of Ukraine in gaining more insight into the event.[6] The events in Ukraine are a reminder that cyber threats are real and that constant vigilance is needed to protect the reliability of the North American

[5] "Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case," SANS Industrial Control Systems and E-ISAC, March 18, 2016.
[6] See ICS-CERT report at https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

grid. At the same time, it is important to note that the operational and technical aspects of the North American BPS are different from those of the Ukrainian system. Other differences include the U.S. industry's mandatory and enforceable cyber security standards, including security management controls and authorized personnel and training controls; network segmentation; and the use of licensed anti-virus software, among other things.

Conclusion

To date, there has not been any loss of load in North America that can be attributed to a cyber attack. At the same time, the security landscape is dynamic, requiring constant vigilance and agility. NERC addresses cyber threats through a comprehensive range of diverse strategies utilizing robust CIP standards, situational awareness, information sharing with industry and government, and strong public private partnerships. NERC remains keenly focused on our mission to assure reliability of the BPS, which is inextricably tied to grid security.

Mr. UPTON. Thank you.
Mr. Aaronson.

STATEMENT OF SCOTT I. AARONSON

Mr. AARONSON. Thank you, Chairman Upton, Ranking Member Rush, and members of the subcommittee. I am glad to be here today to discuss the security of the power grid. We appreciate you holding this important hearing and making it a priority for the subcommittee.

As owners and operators of some of the nation's most critical infrastructure, we share your commitment to ensuring the grid is secure and resilient.

From some of the headlines and movie script scenarios out there you may be left with the impression that a month's-long power outage is inevitable and the power sector is powerless to do anything about it.

If there is one thing you take from my testimony it is this: Our industry is doing an extraordinary amount of work at all levels all the time to defend the grid and to respond to incidents.

You have to remember we live and work in the communities that we serve and our infrastructure is our most important asset. We are motivated for many reasons to make security a major priority.

Since these topics can be sensitive and, as was mentioned, sometimes classified, we may not talk about them a lot in public, but don't take that as complacency or a lack of action.

My written testimony has more extensive details on how electric companies address threats so I won't read it to you. But, instead, I'd like to quickly focus on three areas that form the foundation for how the electric power industry approaches security.

It's three legs of the stool, effectively. So the first leg of the stool is standards. The electric industry has mandatory and enforceable critical infrastructure protections, or CIP, regulatory standards for both cyber and physical security that Mr. Cauley just mentioned.

These are not lax lowest common denominator standards. These are rigorous requirements that improve the industry's security posture.

Failure to comply can cost companies more than a million dollars per infraction per day. So, suffice it to say, companies feel a strong incentive to comply.

But compliance does not equal total security. So that brings me to the next leg of the stool, which is partnerships. 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 am also privileged to serve on the secretariat of the Electricity Subsector Coordinating Council, or ESCC. The ESCC is made up of all three segments of the industry as well as Canadians and independent power generators, the nuclear sector as well as the gas sector.

It is made up of 31 CEOs from across the segments of the industry. Those CEOs meet regularly with senior government officials not to simply update each other but to set a strategic course that has helped the sector make extraordinary advances in grid security

in a very short amount of time by bringing together government-industry executive leadership.

It's also been recognized by the National Infrastructure Advisory Council, which advises the executive office of the president as the model for how critical infrastructure sectors can partner with government.

So the ESCC focuses on four specific areas. The first is deploying tools and technology. The focus here has been moving government-developed tools to industry applications that improve situational awareness. And, again, Mr. Cauley mentioned the best example of this, the Cyber Risk Information Sharing Program, or CRISP.

The second focus for the ESCC has been improving the flow of information. That is making sure the right people are getting the right information at the right time.

From classified briefings for executives to actual intelligence for operators, government and industry are sharing threat information more easily and more often, and some of that has to do with some of the legislation that has been passed by committees like this to make information sharing more seamless between the public and private sectors.

The third thing that we are doing in the ESCC is coordinating with other sectors. While electricity is often described as the most critical to critical, if we don't have water, we can't generate steam or cool our systems. If we don't have transportation or pipelines, we can't move fuel or our equipment. If we don't have communications, we can't operate.

So to address interdependencies, the power sector is working across sectors, and most recently we are pursuing a partnership with the financial services and communication sectors to form a Strategic Infrastructure Coordinating Council, or SICC, that follows the model of the ESCC by bringing senior executives together to form a center of gravity that will help harmonize people, policies, and technologies across the sectors that form the foundation of civil society.

Then the last area of focus for the ESCC also happens to be the third leg of the stool. So we have got regulations, we have got partnerships, and then we are preparing to respond and recover from incidents if there were ever a successful attack. Simply put, electric companies have to be right 100 percent of the time and the adversary has to be right once.

Given those odds, preparing for incidents is just common sense. First of all, we have a history of working together to restore power after an incident through mutual assistant networks where workers from across the sector help affected companies.

We also have a robust spare equipment sharing program including several bilateral and multilateral arrangements, one of them known as the Spare Transformer Equipment Program, or STEP.

We exercise regularly, as Mr. Cauley noted. NERC's GridEx series brings together thousands of operators and executives from across North America in the largest exercise of its kind, and we now are developing a cyber mutual assistance program to coordinate industry resources for companies affected by cyber incidents.

As an example of how quickly the sector can implement new strategies under the ESCC, the CMA program was conceived in

January of 2016, just about a year ago, following GridEx III and the 2015 cyber-attack on Ukraine's energy grid.

In just the last year, this program went from a concept suggested by the CEOs of the ESCC to a program that currently has more than 80 participants and growing almost daily, a legal structure, a play book that has been exercised and even utilized in response to the Mirai botnet that affected internet services this past October.

Bottom line is this: We are constantly working to manage risk, but also planning to address incidents because we understand we can't fully eliminate risk.

There isn't 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 all Americans. From CEOs to operators, the power sector has shown it takes this responsibility very 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.

[The statement of Mr. Aaronson follows:]

STATEMENT OF SCOTT I. AARONSON
EXECUTIVE DIRECTOR, SECURITY AND BUSINESS CONTINUITY
EDISON ELECTRIC INSTITUTE
AND
SECRETARIAT MEMBER
ELECTRICITY SUBSECTOR COORDINATING COUNCIL

BEFORE THE U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON ENERGY

"THE ELECTRICITY SECTOR'S EFFORTS
TO RESPOND TO CYBERSECURITY THREATS"

FEBRUARY 1, 2017

Summary

We depend upon reliable and secure electricity to power our economy and our way of life. Providing this energy and protecting the energy grid against threats are responsibilities that our nation's electric companies take very seriously. Importantly, electric companies understand that they 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, companies follow a multi-layered risk management approach to grid protection known as defense-in-depth.

Under FERC oversight, NERC establishes security standards and regulations that are important to the industry's security posture. In addition to regulations and standards, close coordination and the sharing of threat information between the government and industry help to protect the grid.

The Electricity Subsector Coordinating Council (ESCC), the principal liaison between the federal government and the electric power sector, coordinates efforts to prepare for, and respond to, national-level incidents or threats to electric-sector critical infrastructure. The ESCC focuses on four main areas to improve grid security: Tools and Technology; Information Flow; Incident Response and Recovery; and Cross-Sector Coordination.

Protecting and defending the energy grid against threats are not enough; we also must plan to respond and recover should an incident impact operations.

We also are working to deal with new and emerging cyber threats, such as those potentially associated with distributed energy resources and the Internet of Things.

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 evolving preparedness by applying lessons learned from exercises and real-world events.

Introduction

Chairman Upton, Ranking Member Rush, and members of the Subcommittee, thank you for the opportunity to testify. My name is Scott Aaronson, and I am Executive Director for Security and Business Continuity 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 more than 60 international electric company members, and 270 industry suppliers and related organizations as associate members. For EEI's member companies, securing the energy 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 a member of the Secretariat for the Electricity Subsector Coordinating Council (ESCC). The ESCC is comprised of the chief executive officers of 22 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 incidents 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 initiatives the electric power industry is taking to respond to grid security threats, the value of our government-industry partnership in the face of threats to the electric sector, and the public policy considerations and strategic initiatives that can enhance the cybersecurity of one of the nation's most critical infrastructure sectors.

Managing Risk: An Overview of Threats to Critical Electric Infrastructure

Electric companies understand that reliable and secure electricity is essential to the nation's economy and our way of life. Providing reliable service is a responsibility electric companies take very seriously. Importantly, companies also understand that they 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 known as "defense-in-depth."

The key to this strategy involves setting priorities to protect the most critical energy 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 to meet those threats.

The ESCC is an important partnership that has developed between government and industry to ensure the sector and our nation are secure. Man-made events (such as coordinated cyber and physical attacks) and natural phenomena (like solar flares, major earthquakes, or weather events

on the scale of Superstorm Sandy) require coordination between government and industry, as well as across the critical infrastructure sectors. Every critical infrastructure industry is dependent upon each other to provide services to customers.

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 events in Ukraine, where industry experts accompanied a Department of Energy (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 prepared to manage risk and to respond to all hazards.

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

The electric power sector's defense-in-depth approach to protecting grid assets 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 energy 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 (FERC) 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 that can exceed $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 6 of the cybersecurity standards, and additional modifications are underway to add new requirements mirroring best practices in cybersecurity.

In addition to implementing Version 6 of the cybersecurity requirements, NERC and the industry are developing new requirements to address supply chain cybersecurity. The industry also is implementing new mandatory requirements for physical security as part of the broader suite of NERC regulatory standards.

The industry also uses voluntary standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as DOE's Cybersecurity Capability Maturity Model (C2M2). Electric companies throughout the industry are assessing their

cybersecurity capabilities against this framework and 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 to protect the energy grid.

As 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 who 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, ensure coordination with government on response and recovery efforts, and align messaging.

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

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 in the right way;

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

4. Cross-Sector Coordination: Working closely with other interdependent infrastructure sectors (*e.g.*, communications, downstream natural gas, financial services, water) to ensure all are prepared for, and can respond to, national-level incidents.

Some specific examples of ESCC initiatives within these areas of focus:

Cybersecurity Risk Information Sharing Program (CRISP)

The electric power sector is deploying the Cybersecurity Risk Information Sharing Program (CRISP) to bolster its situational awareness and information sharing. CRISP is a public-private partnership that includes industry, DOE, Pacific Northwest and Argonne National Laboratories, and the Electricity Information Sharing & Analysis Center (E-ISAC), which manages the

program. CRISP seeks to facilitate timely bi-directional sharing of actionable unclassified and classified threat information, using advanced collection, analysis, and dissemination tools to identify threat patterns and trends across the electric power industry. CRISP enables near real-time sharing of cyber threat data among government and industry stakeholders.

Cyber threat information shared through CRISP is helping to inform important security decisions, not just among participating companies but also to all E-ISAC members throughout the electric sector, as information gleaned by the technology is then shared anonymously through the E-ISAC portal. More than 75 percent of all electricity customers are served by electric companies that have deployed CRISP.

Sharing Actionable Intelligence

The electric power industry values its security partnership with the U.S. government. One recent event provides a real-world illustration of how the industry-government partnership works to enhance cybersecurity. In late December 2016, senior DOE and Department of Homeland Security (DHS) officials briefed the ESCC and other energy sector representatives regarding Russian cyber incidents against U.S. private-sector interests. Critical infrastructure sectors—including the electric sector—took immediate steps to review and to secure their systems based on this intelligence. As it turned out, one U.S. electric company discovered a suspected Russian presence on its enterprise network. The company shared this information with DOE, DHS, and all appropriate authorities. Fortunately, no systems responsible for grid operations were impacted.

In this case, thanks to close and ongoing coordination through the ESCC, actionable government intelligence was shared with private-sector operators throughout the sector to better inform their defenses. Electric companies, in turn, continue to share information about compromises with the government to raise awareness of cybersecurity incidents across the private sector and to inform best practices for protection and mitigation.

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, electric companies have 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, and, most recently, following Hurricane Matthew last October. In short, mutual assistance is not just a program, it is in our industry's DNA.

As cyber risks proliferate, the industry, with the ESCC's leadership, moved to develop a cyber mutual assistance program to aid electric companies in restoring necessary computer systems following a regional or national cyber incident. This program builds on the industry's culture of

mutual assistance to develop resource-sharing relationships that can provide surge capacity should a cyber incident exceed the capacity for an individual company to respond.

In addition, electric companies work to maintain and strengthen their ties to state agencies, state and local law enforcement, as well as state Fusion Centers that receive, gather, analyze, and share threat information.

Protecting and defending the energy grid 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.

DOE FAST Act Emergency Authority

Congress took steps to ensure a single government entity would have emergency authority and ultimate responsibility in the event of a true grid security emergency resulting from a cyber attack or other types of intentional or existential threats to the grid. The 2015 transportation bill ("Fixing America's Surface Transportation Act" or FAST Act) provides that, upon a Presidential determination of a grid security emergency, DOE has authority to issue an order for emergency measures to be taken by NERC, a regional entity, or electric sector owners and operators. We commend you for your foresight in addressing this issue, and we are working with DOE to determine the scope and process for such emergency orders. We also appreciate language in the

bill providing liability protections for actions taken in compliance with an order, as well as important protections against public disclosure of sensitive critical energy infrastructure information shared with DOE and FERC.

Spare Equipment Sharing and Transportation

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 two newer industry-led programs, Grid Assurance and RESTORE (Regional Equipment Sharing for Transmission Outage Restoration)—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 have developed a Transformer Transportation Emergency Support Guide to help move these critical assets rapidly in an emergency.

Exercises

Electric companies plan and regularly exercise for a variety of emergency situations—including cyber attacks—that could impact their ability to provide electricity. The largest so far, in

November 2015, was the third biennial industry-wide grid security and incident response exercise known as GridEx III, which 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 energy 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 energy grid.

In its GridEx III After-Action Report, NERC found that, since GridEx II in 2013, industry and government responses to a significant cyber/physical attack continued to improve. The 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 provide a road map for how the ESCC, with input from NERC, and the government should address security issues. GridEx IV is scheduled for November 2017.

Other recent national-level exercises in which the industry has participated include: Clear Path IV, conducted by DOE in April 2016; Cascadia Rising, sponsored by FEMA in 2016; Cyber Guard, a two-week DOD-NSA cyber exercise involving experts from government and the energy, IT, and transportation sectors; and a Treasury Department Joint Financial Services-

Electric Sector Cyber Exercise in August 2016 that examined incident response capabilities and interdependencies between the two sectors.

Supplemental Operating Strategies

One example of "lessons learned" from these exercises and the December 2015 cyber incident affecting Ukraine is a renewed focus on supplemental strategies for operating the energy grid under sub-optimal circumstances. Whether resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary back-up systems, or operating in other degraded states, the industry is working with grid experts to explore "extraordinary measures" that can be anticipated, planned for, and practiced so these are not being contemplated for the first time during an incident.

We continue to plan and move forward to deal with emerging cyber threats.

In addition to the many ongoing industry cybersecurity and resiliency programs, some of which are highlighted in my testimony, the electric sector also is looking ahead to deal with new and emerging cyber issues.

For example, as new distributed energy resources (DER) and behind-the-meter assets have a growing impact on grid operations, new vulnerabilities are created because these technologies are not subject to the same reliability mandates and security requirements that electric companies must meet. Electric companies do not have organizational control over most DER systems, and the customers controlling DER systems do not have a thorough understanding of cyber vulnerabilities or the knowledge and capability to combat cyber threats.

DER may provide an increasing number of potential entry points for access to electric companies' control systems and can affect the operation of the transmission system. DER systems are more reliant on communication and information sharing between grid components, some of which may be open to physical and internet access, making them more vulnerable.

While the promise of DER can increase grid resilience, the integration of these resources at all points in the electric system must be coordinated thoughtfully. The promise of DER and its contributions to resilience require coordinated planning and investments in controls to ensure energy grid operators have visibility into these new resources.

Similarly, the installation of billions of internet-connected consumer devices is another area of potential concern. While devices comprising the "Internet of Things" (IoT) typically are not directly connected to energy grid infrastructure in the same way as DER, electric companies still recognize the risks related to cyber attacks that may seek to leverage the IoT in a way that would impact the energy grid and electric reliability.

The industry already has faced instances of distributed denial of service attacks similar to IoT-leveraged incidents in other business sectors last year. However, these attacks have focused on business systems (such as customer service), and electric reliability has not been impacted. Nevertheless, the E-ISAC and the government share actionable intelligence with the industry and electric companies routinely examine their internet-facing systems for vulnerabilities to ensure that all systems have adequate protections in place.

Conclusion

With exercises and real-world events serving as catalysts 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.

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.

I appreciate the Subcommittee holding this hearing to learn more about cyber and other 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 our nation's electric companies and the government share a sense of urgency, and are working closely in innovative ways to protect critical energy infrastructure from attacks and to limit the consequences of an attack should one occur.

Mr. UPTON. Thank you very much.
Dr. Beck.

STATEMENT OF CHRIS BECK

Dr. BECK. Chairman Upton, Ranking Member Rush and members of the subcommittee, thank you for the opportunity to testify before you today on this important topic.

EIS Council, a 501(c)(3) nonprofit, is, at its core, a public interest organization. Our chief mission is to do our part to ensure societal continuity for black sky hazards by hosting research and national and international collaboration focused on whole community resilience, response, and restoration planning.

Black sky is increasingly becoming a term of art referring to threats that could cause extended and long-duration power outages covering many states and lasting more than a month, and the subsequent cascading failures of our other critical infrastructures.

Six black sky threats have been identified as primary concerns. Three are naturally occurring and three are malicious, including a sophisticated cyber-attack—the subject of today's hearing.

The Ukrainian cyber-attack demonstrated that a blackout of electric power can be achieved through remote cyber means. Stuxnet and Aurora demonstrate that catastrophic damage to physical equipment can be accomplished through cyber-attack vectors on operational technology or industrial control systems, causing disruption, misoperation, or destruction of the hardware they control.

The successful coupling of these two components could result in a black sky event. This would be the case if the damaged equipment were critical to grid operation and required a long period of time to repair or replace.

It would also be the case if the disruption pushes restoration times past the point where cascading failures of other infrastructures began interfering with the restoration process.

In the aftermath of a natural disaster, response activities typically commence once the immediate danger has passed. In a cyber-attack scenario, it is possible or even likely that the attacker could launch subsequent attacks to disrupt response and recovery efforts or cause further damage.

At the same time that the cyber threat is constantly evolving, the attack surface continues to grow with the ever-growing trend to computerize and allow remote access and control.

An adversary may also infiltrate a utility not through a direct attack on the utility system itself, but through a trusted, maybe less secure third party connection, or by inserting malware into critical hardware or software at several points along that product's production life cycle.

Leading power utilities have taken positive action along the cyber-attack threat timeline or kill chain though there is certainly a large spread between the capabilities within the power utilities.

Electric utilities also have a long history of providing mutual assistance, and the same concept is being applied by the ESCC for mutual support in response to cyber incidents though challenges unique to cyber must be taken into account.

Operational technology systems in particular vary greatly from utility to utility. IT and OT professionals are typically a limited resource.

In a large enough attack, availability of such expertise will likely be too limited to address the need, and CEOs may be reluctant to flow personnel to assist others when they might be the next target themselves.

To bolster electric sector mutual support, external support is also necessary. Government support for utilities is available at the federal and state levels. ICS–CERT and E–ISAC provide operational support and information sharing.

A DOD USCYBERCOM may provide assistance through defense support to civil authority missions. DOE is the federal agency for emergency support function 12 for federal support to energy restoration, and the FAST Act provisions now provide broad authority under a grid security emergency declaration by the President.

At the state level, National Guard units may assist electric utilities and state fusion centers in sharing information and including electric utilities in emergency planning and operations.

These support options, however, might be overwhelmed by the scale of the attack. Another possibility would be expanding the concept of mutual assistance to bring IT and OT professionals from other private sectors including information technology, aerospace, water and waste water, telecommunications, manufacturing, and others.

EIS Council is facilitating a process to explore this opportunity. Power grid restoration following a successful black sky cyber-attack will only be possible if broad multi-sector planning is in place for cross-sector support to that restoration process.

Those plans must be continuously tested and improved through exercises such as GridEx and through training within each utility and across sectors. Cyber security enhancements ultimately require focused private and public sector leadership.

When the CEO of a company takes security and resilience seriously, the company develops a culture of security and resilience. Inclusion of security and, specifically, cyber security principles in planning for expansion, equipment replacement and employee training are all essential to enhanced cyber security in the electric power sector.

I thank you very much and look forward to your questions.

[The statement of Dr. Beck follows:]

STATEMENT OF DR. CHRIS BECK
CHIEF SCIENTIST AND VICE PRESIDENT FOR POLICY
ELECTRIC INFRASTRUCTURE SECURITY COUNCIL

BEFORE THE HOUSE ENERGY AND COMMERCE COMMITTEE
SUBCOMMITTEE ON ENERGY

"THE ELECTRICITY SECTOR'S EFFORTS
TO RESPOND TO CYBERSECURITY THREATS"

FEBRUARY 1, 2017

Introduction

Chairman Upton, Ranking Member Rush, and Members of the Subcommittee, thank you for the opportunity to testify before you today on this important topic. My name is Chris Beck, Chief Scientist and Vice President for Policy at the Electric Infrastructure Security Council.

EIS Council

The Electric Infrastructure Security Council, a 501(c)3 non-profit organization, is at its core a public interest organization. Our chief mission is to do our part to ensure societal continuity for Black Sky hazards – those threats that pose the risk of large-area (multiple states to continental in scope) and long-duration (one month or more) power outages, and the subsequent cascading failures of our other life supporting and sustaining critical infrastructures. We do this by hosting research and national and international collaboration focused on whole community resilience, restoration, response and recovery planning. Our programs and projects are intended to help facilitate utilities and other critical infrastructure sectors and their government partners develop

and implement cost-effective, consensus-based resilience and restoration measures by hosting frameworks for sustained coordination, planning, and best practice development. Our flagship program, the EIS Summit Series, hosts annual, international meetings of private sector, government, non-governmental, and academic organizations to further critical infrastructure resilience and whole community preparedness for Black Sky events.

Black Sky Threats Overview

"Black Sky" threats (or hazards) is increasingly becoming a term of art, referring to extreme natural or malicious threats that could cause extended and long duration power outages, covering many states and lasting more than a month. Six Black Sky threats have been identified as primary concerns. Three are naturally occurring: severe regional earthquakes (New Madrid fault), severe (worse-than-Sandy) terrestrial weather, and large geomagnetic disturbances caused by intense space weather. Three are malicious: coordinated physical attack on key electric grid nodes, high-altitude electromagnetic pulse attack (HEMP), and sophisticated cyberattack – the subject of today's hearing. As a further concern, malicious threats could be combined, or deployed at times of severe natural hazards, further increasing their impact.

While important differences exist between these threats, the commonality of their outcome will be power outages of unprecedented scope. For blackouts of this extent, cross-sector interdependencies would interfere substantially with the functionality of normal disaster planning. If we as a nation are to be adequately prepared for such hazards, to preserve the lives

of our citizens and sustain our society, new, well-coordinated approaches to restoration support and emergency planning will be essential.

Black Sky Cyberattack on the Electric Grid

The December 23, 2015 cyberattack on the Ukrainian electric power grid demonstrated that a blackout of electric power can be achieved through remote cyber means. 30 substations were taken offline, resulting in loss of electric power to approximately 225,000 customers, for up to six hours. The affected substations, though disconnected, were not permanently damaged, which allowed for reasonably rapid power restoration.

Once again, more recently, what is believed to be the 2nd cyberattack last year on Ukraine's Bulk Power System took place late Saturday night, December 18, 2016. Automation control systems at Ukraine's northern power substation were disrupted, causing a power outage through much of the northern part of Kiev.

Although these attacks were, thankfully, of limited scope and duration and therefore did not rise to the level of a Black Sky event, both may well have been essentially test cases intended, at least in part, to help perpetrators prepare far more extensive capabilities.

Stuxnet and Aurora demonstrated that catastrophic damage to physical equipment can be accomplished through cyberattack vectors. Both are examples of malware that can take control

of operational technology (OT) or industrial control systems (ICS), and cause disruption, misoperation, or destruction of the hardware that they control.

The successful coupling of such components – gaining control of multiple electric substations and/or generators at multiple locations throughout the country through remote access and then using that access to inflict permanent physical damage on them – could result in a Black Sky event. This would be the case if the damaged equipment were critical to grid operation and required a long period of time to repair or replace, such as large power transformers or generator turbines. It would also be the case if there is sufficient distributed disruption that the needed damage assessment and repair pushes restoration times beyond the point where cascading failures of other infrastructures begin interfering with the restoration.

Black Sky Cyberattack on Multiple Infrastructure Sectors

While cyberattacks on the Bulk Power System could be particularly devastating, there is no reason to believe that a determined adversary would limit an attack to this subsector. While the continued and rapid evolution of cyber threats are making protection continually more difficult, the electric subsector is far better protected than many other infrastructure sectors. Simultaneous attacks on the oil and natural gas subsector, on water systems, communications, government, emergency response, or other infrastructures could both create new categories of severe disruption and seriously complicate power restoration operations.

Special Challenges for Cyberattack Response

In the aftermath of a natural disaster, response activities typically commence once the immediate danger has passed. In a cyberattack scenario, it is possible, or even likely, that the attacker could launch subsequent attacks to disrupt response and recovery efforts and/or cause further damage, using the same attack vector if it is not properly removed from the affected computer systems.

A closely related challenge is the tension between response/recovery and attribution. Identifying and removing malware from an affected system or installing updates or patches will be necessary for recovery to normal operation. Such actions, however, can also overwrite critical data needed for understanding the malware and for attacker attribution.

Evolving Threats and Vulnerabilities

Of all the Black Sky threats, the cyber threat is constantly evolving and therefore very difficult to mitigate or stay ahead of. While the most sophisticated cyberattack vectors may require nation-state level activity, any determined adversary can acquire destructive malware through online criminal marketplaces. Such malware is constantly evolving and can be further modified for novel destructive purposes, and adversaries will continue to seek and develop them to attack U.S. infrastructure assets, among other targets.

At the same time as the threat is evolving, the "attack surface" continues to grow with the ever-growing trend to computerize, automate and allow remote access and control. One such example

is the strong push to update distribution networks through the installation of smart meters, which have the potential to be remotely accessed by adversaries. This could provide a new cyberattack path to the distribution utility. Additionally, if the meters were to be disconnected and destroyed, it could not only affect the homes or businesses whose power would be cut off, but if done on a large enough scale, could cause grid instability due to sudden, unexpected load loss, and require much time and effort to restore.

Another key challenge that is emerging due to the evolving technological and economic landscape is the issue of third-party service providers who have connectivity and access to utility networks. This allows the possibility for an adversary to infiltrate a utility not through a direct attack on the utility's system itself, but through a trusted but less secure third-party connection. In addition, in our evolving global supply chain, malicious actors have opportunities to insert malware into critical hardware or software at several points along a product's production lifecycle. Furthermore, third party vendors may have access to or hold sensitive utility data. If compromised, this data can provide an adversary with a roadmap – designs, blueprints, operational data – for attacking the utility.

Enhanced Planning for Electric Subsector Response and Recovery

The cybersecurity challenges are daunting, but electric power utilities are taking important steps to addressing this ever-evolving challenge. The largest and most sophisticated utilities are achieving cybersecurity enhancements nearly on par with the banking sector, which has the longest history of understanding and addressing security threats, including cyber threats.

To effectively respond to cyber incidents, it is critical to ensure that utilities and responsible government agencies have robust plans and procedures for critical response activities, communication, and partnership. Such plans and procedures must be vigorously exercised and constantly updated and improved, to keep pace with the threat. The GridEx series, hosted by NERC, is a good example – a biennial exercise of increasing difficulty and complexity, intended to push the system past the "breaking point", then gather lessons learned to improve planning for better protection and faster restoration of the system in future.

The leading power utilities have taken positive action along the cyberattack threat timeline or "kill chain". Primary control centers' physical and IT infrastructures have been hardened to resist attack, and their networks are constantly monitored and scrubbed of malware. Robust backup control centers that can operate the utility system if the primary has been successfully attacked are in place. Secure, clean copies of IT and OT software are held and ready for rapid installation to respond and recover from successful attacks. "Spare tire" operational modes – initiated by the North American Transmission Forum – that do not offer the full functionality of regular operations but that allow limited, critical operations to continue during response and recovery activities are being developed and implemented. Utilities must also maintain the ability to use mechanical controls, through regular training. There is certainly a large spread between the capabilities of the most sophisticated and forward-leaning companies and others that are not as well capitalized or fully appreciate the threat, but these represent the current best practices.

While robust plans and procedures to enhance the resilience of individual utilities is a critical component, a sophisticated, Black Sky level cyberattack would affect several hundreds or even thousands of locations nearly simultaneously, and without warning. In the interconnected grid, the successful disruption of utilities that were unable to defend against the initial attack will likely shut down, and these can cause the cascading blackout of even those utilities that were prepared for attack. To effectively respond to such a crisis, enhanced partnerships between utilities themselves, utilities and government agencies, and across infrastructure sectors will be important.

Electric utilities have a long history of providing mutual assistance, as we witnessed during Superstorm Sandy and many other natural disasters. The same concept can be applied for mutual support in response to a cyber incident, though challenges unique to cyber need to be taken into account. The mutual assistance provided during Sandy was primarily focused on repairing, replacing, and reconnecting downed power poles and lines, a standard practice across the country. In contrast, while every utility has IT and OT systems, OT systems in particular vary greatly from utility to utility, and so are much less "standard" than poles and power lines and the tools needed to repair them. On a positive note, an inherent security benefit of this non-uniformity of OT systems makes it less likely that any one piece of malware could successfully infect and attack all OT systems. The challenge from the mutual assistance perspective for recovery is that a utility that intends to help another may not be able to, or could possibly even cause further harm if they were to take well-intended but improper action on an OT system.

That said, there are options for cyber mutual assistance, a concept and practice introduced and being driven by the Electricity Subsector Coordinating Council. Moving along the spectrum from least to most difficult, assisting utilities who can provide IT expertise to a compromised utility can assist with cleaning, repairing, and restoring the afflicted utility's IT system, thus freeing up the affected utility's staff to focus on OT issues. They could also help with recovery and attribution by reviewing network logs to find malware signatures or other anomalies. If attacks are ongoing, they may be able to support active perimeter defense activities. Finally, if either a common OT system is identified between utilities, or, more likely, pre-event cross-utility training on each other's OT architecture is done, a supporting utility could directly assist in OT restoration.

IT and OT professionals, however, are typically a limited resource. In a large enough attack, availability of such expertise will likely be too limited to address the need. In addition, especially given the problem of sustained or follow-on cyberattack, CEOs may be reluctant to flow critical personnel to assist others when they might be the next target. To bolster the intra-electric sector mutual support, external support is also necessary.

Government support for utilities is available at the Federal and State levels. Federal resources include the DHS Industrial Control Systems Computer Emergency Response Team (ICS-CERT) teams to provide focused operational capabilities including system analysis and advice on mitigating ICS compromises, and the Electricity Information Sharing and Analysis Center (E-ISAC) to provide information on emerging and evolving threats, and their mitigations. Within

the Department of Defense, USCYBRERCOM is analyzing its ability to provide support to utilities under Defense Support to Civil Authorities missions. In addition, they recognize that because CONUS military installations rely on civilian electric power grids, adversaries can attack and weaken U.S. military power by going after the supporting electric infrastructure. Finally, the Department of Energy is the Federal coordinator and primary agency for Emergency Support Function 12 (ESF 12), the primary mission of which is to facilitate the restoration of damaged energy systems. In addition to authorities under ESF 12, key provisions of the Fixing America's Surface Transportation (FAST) Act of 2016, provide the Secretary of Energy with broad authority to issue emergency orders for electric grid protection and restoration if the President declares a "grid security emergency", which includes the occurrence or imminent danger of a cyberattack.

At the State Level, a growing number of National Guard units are developing expertise and programs to assist electric utilities in combatting cyberattacks. State fusion centers are also providing information on cyber threats, and a growing number of states recognize that electric power and other utilities must be involved in emergency planning and disaster response operations.

However, for a large scale attack these options, taken together, might be overwhelmed by the scale of the attack. Another possibility that may be helpful would be expanding the concept of Mutual Assistance, to develop a mechanism to assist corporations in bringing in IT and OT professionals from other private sectors resources. This could include arranging for participation

by corporations in many fields, including information technology, aerospace, water/wastewater utilities, telecommunications, manufacturing, and others. Many aerospace companies, for example, have established cybersecurity business divisions within their companies.

To make use of these potential resources for a major disaster, new best practice approaches could be developed for implementation by those power companies that wish to provide certification and periodic training of supplemental, volunteer engineering and technical teams for preplanned support to internal corporate IT and OT professionals. EIS Council is facilitating a process to explore this opportunity, working with interested power industry and external, private sector providers, as part of a Certified Power Recovery (CPR) Engineering Team Initiative.

Overall, cybersecurity protection enhancements really require continuing evolution of both private and public sector leadership, addressing this threat diligently, and continuously. Security has not traditionally been a high priority item within many infrastructure sectors, including electric power. That has certainly changed dramatically in recent years, but continuation of the trend to address cyber security throughout the nation's large and diverse energy sector, at the highest levels of decision making, is necessary to ensure that cyberattacks can be addressed. To cite one important example, the Electricity Subsector Coordinating Council (ESCC) is a public-private partnership between leadership in the Federal government and CEOs of electric power utilities. The ESCC is focused on protecting our grids from national-level security events, which includes cyberattacks. When the CEO of a company takes security and resilience seriously, the company develops a culture of security and resilience. Inclusion of security, and specifically cybersecurity principles in internal planning for company expansion, equipment replacement,

and employee training are all essential to promote the most cyber secure electric power sector we can.

Enhanced Planning for Cross-Sector Restoration Support

While there are many challenges associated with the evolving needs for cyber protection, the electric subsector, in particular, is already a leader in addressing these issues. However, another and perhaps even greater challenge must be addressed, if we wish to be prepared for the multi-sector coordination challenges that would be presented to power restoration teams if a cyber-attack – in spite of protection measures – proved successful.

Once a power outage exceeds a critical threshold – perhaps several days, for example, emergency generators in many interdependent infrastructure sectors will run out of fuel. Today there are not yet adequate plans to provide for extensive resupply of such fuel – or of burned-out generators – in an environment with severely disrupted communications, transportation, and limited and failing lifeline infrastructures. As a result, the processes power companies typically have in place to deal with severe emergencies will face unique challenges, including "black start" procedures designed for restarting grid segments without outside power.

Power grid restoration following a successful cyber-attack will only be possible if extremely broad multi-sector preplanning is in place to provide for cross-sector support to that restoration process, to coordinate the support that these other infrastructure partners will themselves need in

this environment, and to save and sustain lives during an extended restoration process. EIS Council's EPRO SECTOR initiative is hosting a coordinated planning process to address this need. This initiative is hosting planning by leaders of a wide array of interdependent sectors, as they utilize this framework to help define, detail and implement cross-sector coordination processes that will be needed in Black Sky scenarios. Best practice information is also gathered and shared through EIS Council's EPRO Handbooks and Black Sky Playbooks. Handbook I focuses on the Electricity Subsector and Whole Community Preparedness. Handbook II is a two-volume resource that focuses on the Fuels and Water/Wastewater Sectors. Handbook III, currently in development, will put a special focus on cross-sector cooperation for restoration activities. The Black Sky Playbooks are specific to each sector, but also include cross-sector planning through the identification of "external requirements" – assistance needed from other sectors and government agencies to prepare for and respond to Black Sky hazards.

By its nature, this process must provide for ongoing, operational, coordinated planning by a wide array of public and private sector corporations and agencies. Many streams of parallel meetings are now going on throughout the year, designed to host cross-sector planning by many sectors, to include energy, water, food and pharmaceutical production and distribution, health care, communication, transportation and both state and federal agencies.

This process is truly vital, if societal continuity is to be ensured to address, not simply a possible successful cyber-attack, but for any Black Sky hazard. Our purpose and role in hosting this uniquely broad EPRO SECTOR process is simply as hosts and facilitators. However, I would

like to publicly express our thanks to the remarkable, high level participation of senior leaders from many sectors already involved in this complex and expanding process.

Conclusion

A sophisticated, distributed cyberattack on IT and OT systems within the electric power sector is one of the six Black Sky threats that could cause widespread and long-term power outages within the United States or anywhere in the world. Of the Black Sky threats, it is the fastest evolving and the most difficult to stay fully abreast of.

Effective protection and response for a cyberattack will require diligent effort by the entire electric sector, and by their partner sectors. Protecting and restoring utility OT systems is challenging, because each utility has its own architecture design, which can include unique protocols and legacy equipment that may be years old.

If, in addition, we wish to ensure national and societal continuity in the aftermath of a successful cyber-attack, unprecedented, broad and well-coordinated planning is required, not just for electric utilities, but by a wide array of other infrastructure sectors, and governments at all levels.

In summary, proper prior communication, coordination, information sharing and cross-training is enhancing the security of our Nation's electric grid, and by extension, our Nation as a whole, and

the power industry is a leader in this domain. Those efforts, however, must be continually expanded and strengthened, as the cyber threat continues to evolve. To address the full ramifications of this hazard, broadly coordinated public and private sector planning is needed that goes far beyond the electric subsector.

Mr. UPTON. Thank you.
Ms. Sugg.

STATEMENT OF BARBARA SUGG

Ms. SUGG. Good morning, Chairman Upton, Ranking Member Rush and all members of the Energy Subcommittee.

My name is Barbara Sugg. I am the Vice President of Information Technology and Chief Security Officer at Southwest Power Pool, which is headquartered in Little Rock, Arkansas.

Southwest Power Pool is one of the nine independent system operators and regional transmission organizations—the term ISO/RTO will be used henceforth—in North America.

Collectively, these nine organizations serve two-thirds of the energy consumers in the United States and half in Canada. We are nonprofit organizations. We do not own generating plants or operate generating plant substations or transmission facilities.

However, we do provide a number of various services from reliability coordination and balancing authority functions to transmission planning for future expansion of the transmission grid.

We all have the common goal of ensuring sustainable, affordable, and reliable power with our wholesale energy markets.

I am here today on behalf of the ISO/RTO Council, known as the IRC. The IRC has an executive committee, which includes the CEOs from each of these nine organizations and is made up of a number of committees and working groups focused on different areas of interest to the ISO/RTO community.

I serve as a member of the IT committee, which brings together the chief information officers from each of those nine organizations, where we come together to share best practices, to collaborate on common interests, and to work on directives that may come from the executive committee.

One of the working groups that reports to us is the security working group. With this security working group, which has been in place for a very long time now, there are security experts that come together from each of our regions to share best practices, to work on incident response planning, and to understand our dependencies with each other.

Cybersecurity is a top concern at the ISO/RTO. As Ranking Member Rush said earlier, it's not a matter of if but when, and we recognize that.

We have five core strategies to our cybersecurity framework. One of those is defense. Certainly, we have to be prepared to defend against attack. We do this through controls, through multiple layers of security and good practices to ensure that we stand ready to defend.

The next is response. From advanced security monitoring and practicing incident response plans we stand ready to respond. And the third is recovery. You've heard us mention about the GridEx opportunities to practice our recovery drills.

We do those every other year in a nationwide effort but we also do local, state, and regional exercises much more frequently to ensure that our recovery plans are ready to go.

Partnership is the fourth key element of our strategy and these gentlemen talked a lot about all the of the information-sharing op-

portunities and the various government agencies that work with us to collaborate and provide cyber assistance.

The fifth is education. We recognize the importance of every single ISO/RTO employee when it comes to protecting our systems and protecting our information, and so security awareness is high on our list.

Over 10 years ago, the CIP standards to critical infrastructure protection standards came out. They've advanced quite a bit over the last decade and they serve as a base level of security for us.

However, we have to get beyond the standards and recognize that a culture of compliance is important but even more so important is a culture of security.

We look beyond the standards in a number of ways from developing, in advance of standards, security coding requirements for our control system vendors. And when I say we I am talking about the entire ISO/RTO community working together to make sure that we are equally protected.

We have worked with the FERC energy infrastructure security office to do security architecture reviews, and to look for best practices and talk about evolving threats and current technologies.

It's very difficult for the standards to keep up with the evolving threats and so we must look beyond that. It's also difficult with emerging technologies.

Standards shouldn't be so prescriptive that they limit us in our capability to develop new infrastructure and new architecture. And we work very closely with NERC and the rest of the community to ensure that those standards are secure enough for us without being overly prescriptive and limiting our capabilities to keep up with the evolving threats.

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

[The statement of Ms. Sugg follows:]

Testimony of Barbara Sugg

Vice President of Information Technology and Chief Security Officer

Southwest Power Pool, Inc.

Member, Information Technology Committee, ISO/RTO Council

Before the House Committee on Energy and Commerce

Subcommittee on Energy

"The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

February 1, 2017

Executive Summary

- ***ISO/RTO Council (IRC):*** The IRC is made up of nine Independent System Operators and Regional Transmission Organizations (ISO/RTO) in North America serving two thirds of electricity consumers in the United States and over half in Canada. The IRC and its committees bring together representatives from each ISO/RTO to work together to match power generation instantaneously with demand to keep the lights on and ensure access to affordable, reliable and sustainable power via wholesale energy markets.

- ***CIP Standards:*** The Critical Infrastructure Protection (CIP) Standards have been maturing since first approved by the Federal Energy Regulatory Commission in 2008. These mandatory standards provide for a robust, base level of security for which all utilities, including ISO/RTOs, must adhere. The CIP Standards cover numerous domains of cybersecurity, including, but not limited to, identifying cyber assets, controlling access, managing changes, addressing vulnerabilities and protecting information.

- ***Culture of Security:*** Each ISO/RTO acknowledges cybersecurity as their top corporate risk. Our core cybersecurity strategies focus on the key principles of Defense, Response, Recovery, Partnership and Education. Our security programs must continue to reflect more than that which is required by the standards.

- ***Defense in Depth:*** The IRC is committed to collectively supporting the resiliency efforts of each ISO/RTO. While system redundancies are necessary requirements, ISO/RTOs also maintain close ties to the utilities they serve, as well as their neighboring regions thus allowing for immediate operational assistance and threat mitigation in the event of a cyberattack.

- ***Response, Recovery, Resilience:*** ISO/RTOs routinely practice cyber incident response and system recovery to ensure resilience in the wake of a cyberattack. Drills are routinely conducted on local, state, regional and federal levels, in coordination with government agencies and industry associations to provide opportunities to improve our ability to respond and recover with the goal of maintaining the highest possible level of resilience.

- ***Conclusion:*** It is essential that the electric industry continue to prioritize cybersecurity maturity above and beyond that which is required for compliance as the evolving threats and emerging technologies are surfacing faster than standards can be contemplated and promulgated. While the standards themselves are indeed robust, we must not be complacent in our efforts to protect the bulk electric system from cyberattacks and must continue to maintain reliability and resiliency for the American people.

Good morning Chairman Upton, Vice Chairman Olson, Ranking Member Rush, and members of the Subcommittee. Thank you for holding this hearing concerning the electricity sector's efforts to respond to cybersecurity threats. My name is Barbara Sugg and I am the Vice President of Information Technology and Chief Security Officer at Southwest Power Pool Inc. (SPP) headquartered in Little Rock, Arkansas. SPP is one of nine Independent System Operators and Regional Transmission Organizations (ISO/RTO) in North America that make up the ISO/RTO Council (IRC), established in 2003. I am testifying before you today, as the designated representative of the IRC, about the requirements and responsibilities of ISO/RTOs in protecting the bulk electric system in North America from cyberattacks, as well as responding to and recovering from such an event.

The IRC serves two-thirds of electricity consumers in the United States and more than half in Canada, spanning three interconnections. ISO/RTOs match power generation instantaneously with demand to keep the lights on and ensure access to affordable, reliable and sustainable power via wholesale energy markets. ISO/RTOs provide a variety of services to their diverse groups of members, including serving as North American Electric Reliability Corporation (NERC) certified Reliability Coordinators, Balancing Authorities, transmission planners, open access transmission tariff administrators, and wholesale energy market operators.

By sharing innovative ideas and best practices, IRC members work together to build a smarter and more efficient and secure electric grid that is well prepared to serve the North American power market and its consumers, today and in the future. As a collective group, the IRC consists of an Executive Committee, comprised of the chief executive officers from each ISO/RTO, as well as numerous committees responsible for supporting the IRC's goals and initiatives. These

committees share information across a wide range of important areas, including potential physical and cyber threats, regulatory and legislative issues, standards development, transmission planning, market standardization and information technology. Across the numerous IRC committees, staff from each ISO/RTO routinely work together in a collaborative, open and transparent manner within the framework established by the IRC.

For the past nine years, I have served as a member of the IRC's Information Technology Committee (ITC) alongside senior IT executives from each of the ISO/RTOs. The ITC shares expertise and advice on existing IT functions and current activities within the wholesale electric industry and makes recommendations for IT standardization and architecture. The ITC has established a Security Working Group (SWG) to coordinate and communicate areas of mutual concern with regard to the development of applicable cyber and physical security practices. The SWG facilitates interactions among its members and collaborates to identify security issues and solutions.

Cybersecurity is a top priority throughout the industry, and the IRC is committed to collectively supporting the resiliency efforts of each ISO/RTO and advancing the cybersecurity posture of the power grid. Additionally, we have and will continue to partner with local, state, regional and federal governments, NERC, the Electric Sector Coordinating Council (ESCC), utilities and academia to stay ahead of the continuously advancing threats. Our core cybersecurity strategies focus on several key principles:

- Defense: Ensuring that we have the adequate controls and good security hygiene in place to prevent attacks.
- Response: Providing advanced security monitoring to correlate events and see patterns and indicators of compromise.

- Recovery: Maintaining continuity plans, exercises and drills to quickly recover critical systems in the event of a significant cyber event.
- Partnership: Coordinating with industry and government agencies before, during and after an event through the Electric Sector Coordinating Council (ESCC).
- Education: Recognizing the importance of every ISO/RTO employee in keeping the enterprise secure.

More than a decade ago the need for cybersecurity standards became evident as malicious activity was becoming more frequent and potentially destructive. Even with a dedicated collaborative focus on cybersecurity in the electric industry, standards were needed to address critical risks and ensure that all entities across the industry were appropriately protected and prepared. Developed by industry experts and facilitated by NERC, Version 1 of the Critical Infrastructure Protection (CIP) standards were approved by the Federal Energy Regulatory Commission (FERC) in 2008, making compliance with these standards mandatory and enforceable. Noncompliance could result in penalties as high as $1 million per day per violation.

Since first approved by FERC, the standards have been expanded to include all bulk electric system assets and their related cyber assets. Version 5 of the CIP standards became enforceable in July 2016 and consists of 11 different standards and approximately 110 sub-requirements for which we must each comply. These standards cover a wide range of risk areas from identification and classification of cyber assets to physical security, personnel and training, event monitoring, communication, incident response, protection and isolation of network architecture, access and change control, and system recovery. Though the CIP standards are continuing to evolve and mature to cover areas such as protecting our supply chain, the standards serve as robust, base-level requirements for securing our critical infrastructure. As an industry, we must

maintain the flexibility and adaptability to implement the latest technological advances in securing our infrastructure. We must look beyond the standards as we secure the bulk electric system.

The IRC committees and working groups communicate and coordinate with organizations such as NERC's Electricity Information Sharing Analysis Center (E-ISAC) and local, state, regional and federal agencies, including the FBI and Homeland Security, to ensure that all ISO/RTOs are secure and prepared to act in a cyber emergency. Under the direction of NERC, coast-to-coast drills, referred to as Grid Ex, are conducted biannually to give all utilities opportunities to coordinate their response to simulated cyber and physical attacks on electric and other critical infrastructures across North America. Local, state, regional and federal government agencies, including the FBI and Homeland Security on the federal level and appropriate state and local agencies with which the ISO/RTOs closely coordinate on cybersecurity matters, as well as ISACs and supply chain organizations, are involved with the planning and execution of Grid Ex. Grid Ex IV is scheduled for this November. On a more frequent basis, individual ISO/RTOs are routinely involved in regional or statewide exercises conducted throughout North America, thus ensuring opportunities for organizations to verify their readiness to respond to and recover from cyber and physical attacks.

Though compliance with the CIP standards is mandatory and audited, with violations resulting in potential fines, the culture throughout the electric industry is maturing from one of compliance to a culture of security. A key element in the protection of our critical infrastructure is our implementation of multiple layers of security, known as a defense-in-depth strategy. While system redundancy is critical, ISO/RTOs also maintain close ties to the utilities they serve. If cyberattacks were successful on an individual ISO/RTO's critical infrastructure, neighboring

ISO/RTOs as well as member utility companies would immediately take action, assist with continuous operations and help isolate the attack to minimize any impact to the bulk electric system. Exercises such as Grid Ex give ISO/RTOs and their member utilities prime opportunities to practice their defense-in-depth strategies.

Additional developments in the electric utility industry to assist with resiliency include programs such as the Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP) which gives participating utilities early warning of potential cyberattacks. The ESCC has developed a Cyber Mutual Assistance (CMA) Program that provides emergency assistance, in the form of services, personnel or equipment, to participating entities in advance of, or in the event of, a disruption of electric service, systems or IT infrastructure due to a cyber emergency.

I speak on behalf of all of the ISO/RTOs in North America in stating that we are focused and committed to continuing to advance the security of the power grid and will continue to partner with local, state, regional and federal government agencies, NERC, the ESCC, utilities and academia to stay ahead of the continuously advancing and evolving threat. We must also remain involved in the development and implementation of regulations and standards to ensure that they allow for the flexibility needed to meet the security challenges we face in continuing to provide reliable, affordable electricity to consumers. It is essential that the electric industry continue to prioritize cybersecurity maturity above and beyond that which is required for compliance as the evolving threats and emerging technologies are surfacing faster than standards can be contemplated and promulgated. While the standards are indeed robust, we must not be complacent in our efforts to protect the bulk electric system from cyberattacks and must continue to maintain reliability and resiliency for the American people.

Mr. UPTON. Well, thank you all.

I think each of you mentioned that it is a daunting task. When you look at the power grid, 7,700 operating power plants that generate electricity from a variety of primary energy sources, 200,000 miles of high-voltage transmission lines, 55,000 substations, five-and-a-half million miles of local distribution lines.

I think each of you mentioned that you have to be right every day. They just have to be right once for a catastrophe to happen. And as we all know, we passed, on a bipartisan basis, the FAST Act in the last Congress.

Tell us how that has helped you on a bipartisan basis. Tell us specifically, Mr. Cauley and Mr. Aaronson, how has that helped protect consumers?

Mr. CAULEY. Well, thank you very much for the question, Mr. Chairman.

Two ways for me in particular. One is there was a lack of clarity around emergency authorities and I think providing those emergency authorities to the Department of Energy under an emergency declared by the President was helpful.

I testified a number of times in the past about that potential gap. I think the other thing that's extremely valuable to us and to consumers is it provided for greater protections of cybersecurity information.

It's very important that as companies report to us details that border on being classified, if not classified, that we are able to maintain the confidences and keep that secure. Particularly, allowing FERC to have procedures to secure information which we frequently exchange with them, but other controls around maintaining those confidences.

Mr. UPTON. Mr. Aaronson.

Mr. AARONSON. Echoing some of the things that Mr. Cauley just said, agree. And then in addition, I think it really speaks to the value of the partnership at a very high level, providing the Secretary of Energy, who oversees our sector-specific agency with some authorities in the midst of a grid security emergency, which was very well defined in the FAST Act.

Further, it sort of solidifies that relationship in the midst of an incident. And the fact that it calls for coordination with the sector—where practicable—during such emergency ensures that the Secretary would be well informed on what to order.

We are in the process of responding to the notice of proposed rulemaking from the Department of Energy that would outline some of the processes for how this authority would be used and we look forward to continuing that conversation. The joke has come up—there isn't one phone number you can call, the Batphone, for the electric sector.

So having a understanding of who would need to be coordinated with and contacted in the midst of such emergency is going to be a challenge.

But, again, with the Sector Coordinating Council playing that role as a center of gravity with the ISO/RTO Council and other partners throughout the sector it gives us a good, high level set of entities to coordinate with should the unthinkable happen.

Mr. UPTON. Mr. Cauley, you talked a little bit in your testimony about the tabletop exercise. Can you elaborate a little bit more?

The other thing I want to hear particularly, Mr. Aaronson, from you, as it relates to that, and I presume that you were involved, the STEP program.

One of the concerns that a number of us have raised is if there was some issue where a transformer was taken down because of the lack of uniformity between a variety of different units that may be taken out of business. How long would it actually take to get new transformers into place and the mechanism that that would go about it?

I presume that that was probably one of the issues that was engaged in a tabletop exercise that you had.

Mr. CAULEY. The exercise in preparing for our fourth, now in November of this year, have intentionally gotten progressively more difficult and challenging to overcome, and the pattern is we build capability, we learn what we learn, and we get better each time.

I think as we run the exercise in a way that's two days and that it's companies distributed across the U.S. and Canada participate locally in their state and local environment using their operating systems and people. People actually run out to stations.

They call the FBI. They actually do it on the ground. Then there is a central exercise that we look at at the executive level with the top levels of government, and we have had FEMA, DHS, White House representatives and others.

Mr. UPTON. Are the results of that in a classified setting?

Mr. CAULEY. There is a public report for each of the exercises. What we found is that when we propose an exercise that destroys equipment, explosions, deaths, where the power could be out for weeks and potentially months, it really exceeds the capabilities that we have anticipated in the past, not just industry, but government. We never thought of it that way.

We have to think differently in terms of unity of effort, how do we unite around these capabilities and bring the best of industry, best of government to overcome those situations.

Mr. UPTON. I know my time is expired, but I have one quick question on that. Were the governors engaged in this tabletop exercise?

Mr. CAULEY. We anticipate expanding that in GridEx IV in November but, yes, there were representatives from National Guard. The state of Wisconsin, I believe, was represented. And so we did engage some state-level representation at the table.

But, obviously, we need to bring in a lot of state-level activity. A lot of the solution, in my mind, is going to be how do we handle the public situation and the issues on the ground during a crisis. And that really involves local and state governments to support it.

Mr. UPTON. And Mr. Aaronson, just quickly to respond on the STEP program.

Mr. AARONSON. So I appreciate you asked that. In addition to STEP, let me kind of go through a few of the resiliency programs.

This goes to some of the things Gerry was just talking about with respect to having an exercise, understanding where your vulnerabilities are, and then implementing some solutions to fill those gaps.

In addition to this Spare Transformer Equipment Program which grew up about 10 years ago, a little bit more than that, that is a binding relationship between the companies that are a part of it.

In the event of a presidentially-declared terrorist incident, there is a contractual obligation to share equipment during such incident. That's a really high bar.

Fortunately, STEP has been utilized beyond just in presidentially-declared terrorist activities but to be able to move these really important components that form the backbone of the system.

In addition to STEP and its rigorous approach to Spare equipment, we also have something called SpareConnect, which is effectively a database of asset owners and asset managers for companies.

If I am a company that has been impacted by something and I need to get one of these high-voltage transformers in place, I can create a bilateral agreement, call the person who has the equipment that I need, make an arrangement, and have it moved into place.

There also are industry-led versions of this, something called Grid Assurance that has stood up. Again, companies come together to pool resources and a new program called Restore, which is a regional approach, along the same lines.

Last thing I'll say about this is having the equipment is one thing. Moving it is another. These things are quite literally hundreds of thousands of pounds and very hard to move. It has required us to work with other sectors, again, going to interdependencies across sectors, but rail and trucking in particular and then the riggers who actually get it onto the rail car, move it into place and then go the last mile to bring it to the location.

We have both worked with the rail industry and exercised it through something called the Transformer Transportation Working Group. So, again, lessons learned from all of these incidents have really informed industry programs that are making us more resilient and more able to move equipment to where it's needed.

Mr. UPTON. Sorry it took so long. Thank you.

Mr. Rush.

Mr. RUSH. I want to thank you, Mr. Chairman.

I want to touch on an area that we have been silent on—this hearing's been silent on so far and that's the area of the cybersecurity workforce.

I think that's a very critical concern on the plans or the technology—on the well-intentioned efforts of many of us we have come to know and we don't have a sufficient, capable, and expert workforce.

According to the IEEE, there are a million unfilled cybersecurity engineering jobs around the world with that number expected to grow by 1.5 million by 2019. In the U.S. alone there are only 67 job seekers for every 100 open cybersecurity positions.

I am wondering if this shortage of available workers is posing problems for electric companies seeking to fill cybersecurity jobs that protect our electricity grid.

Mr. Aaronson, can you talk about the current situation in the electricity sector as it relates to cybersecurity jobs and is it indeed

true that companies are finding it difficult to find and hire skilled workers to fill these positions?

Mr. AARONSON. So I think this is a refrain that you'll hear, and I am sure there is others on the panel who have some experience actually trying to fill these positions.

I will say I've heard from my membership and across the sector that this is a challenge. There are a lot of needs and not a lot of people to fill it.

This is something that's going to require a long-term concerted effort starting with STEM education and moving up to attracting a workforce to this particular critical infrastructure industry.

I will say a couple of things. EEI in particular has a program known as Troops to Energy, and that helps to take people who have served in the military who have excellent skill sets and really do lend themselves to being a part of a critical infrastructure industry.

So there is attraction there. There is also attraction among cyber workforce and cyber experts. This is a pretty cool industry to be in. You are the most critical infrastructure sector and we are quite literally defending against adversaries from near pure nation states all the way down to sort of the traditional proverbial hacker kid in his mom's basement.

Having that opportunity is something that is attractive but it doesn't change the fact that we need to generate more of these people.

Mr. RUSH. Ms. Sugg, would you want to add anything additionally?

Ms. SUGG. That's a great question and an interesting topic. I don't find that we are having as much trouble filling those kinds of positions because we are working with the universities.

STEM education is a big focus for us as well. At the university level we are working with a number of them on their curriculums, and what's interesting is the Millenials are particularly skilled at this.

This is new technology. It's evolving threats and it's something that the Millenials find really exciting and some of our most innovative thinkers, which is really what you need to think outside of the box on security, are coming out of the universities.

There are a number of opportunities for experienced employees to get education and certifications in cybersecurity areas.

So that's been helpful as well and it is something people that have worked in other areas find interesting and perhaps want to change their careers because it is ever changing and good employees love a good challenge.

The universities are producing some really skilled graduates that challenge our way of thinking about security in a very healthy way.

Mr. RUSH. Is there a role for the federal government in terms of increasing the quality and quantity of the cybersecurity workforce?

Ms. SUGG. I think there is an opportunity for the federal government to challenge the universities to think more broadly about the different types of cybersecurity in areas and sectors that are perhaps less secure, such as the internet, and maybe there are opportunities to fund research toward developing a more secure internet

and that would be something that would be very interesting at the academic level.

Mr. RUSH. I want to thank you, Mr. Chairman. I yield back.

Mr. UPTON. Thank you. The chair would like to recognize the chairman of the full committee, Mr. Walden, for 5 minutes.

Mr. WALDEN. I thank the chair and thank our witnesses again for your testimony and your counsel.

I listen to this and I think about your tests. I was in the radio business. We would do these emergency alert tests and drills from time to time, and we had one of these. You were talking about how you go out to the substation, you call the FBI, you do all that. We got the call into the radio station to announce that Bonneville Dam, one of the major dams crossing the Columbia River, and we were supposed to announce on air had been breached.

Fortunately, I had a sort of retired announcer working that Saturday morning who said, "I think it's probably not a good idea to actually go on the air and tell people that one of the Columbia River dams has been breached, but we will make a note here."

So you have to be careful when you do these exercises, but they are really important because emergencies do happen. I think back to what happened during Hurricane Katrina and how rapidly things disintegrated when there was no power. Because then there is no water, there is no sewage, there is no refrigeration. The ATMs don't work.

I talked earlier about how we are all connected to these digital devices. You can't talk to your loved ones. You can't make emergency calls. So the work you're doing to push this and test this is really important.

I know many of us have been in both classified and unclassified briefings on this matter about the reliability of the grid and the threats that are there. We are very cognizant of the cyber security issues, and the attempts by others to put hardware into our systems that have vulnerabilities in it, and to harness the internet of things to be a swarming attacking machine, basically.

When you analyze the systems that are there, and I don't mean the hardware systems—I mean the human systems to communicate and interact—what are we missing? What are you finding we need to improve on?

Are you hamstrung by certain laws, too? We did six hearings, I think, on our telecommunications subcommittee on this topic of cybersecurity. Every witness on every panel said please do no harm.

If you lock things in statute in terms of technology the bad guys will know what we have to do and you'll misallocate our capital. Are there things like that locked in that we should review, either in a public setting or in a more secure setting?

We want to make sure we have a reliable grid that can withstand any kind of issue whether it's a solar flare or a bad actor. What are we missing here? Or is it all perfect?

Mr. CAULEY. Well, I'll just start the response. I think a lot of the framework that we have is really good. I think the idea of the industry participating in a standard setting and the standards being really focused on being adaptive and sort of driving solutions I think works.

So I think continuing to engage industry experts and leaders, and the process that we have to Section 215 in FERC and NERC I think is very helpful.

There are some challenges that are difficult. Most of the challenges that we face are not limited to the electric system and I think, once we start talking about the kinds of existential threats that we are thinking about here, revolving a broad sweep of telecommunications and other industries, finance and others, I don't ever expect there is going to be an attack that's just only on the grid.

So I think the ability to work cross sector and to engage multiple sectors together in a conversation and leadership is very helpful. I think we are challenged with supply chain and sort of the global picture that everything that we get and use from the system that's digital is coming from somewhere in the world is a challenge.

And the final thing I would say that we need to continue to work on together is strategic reserves around essential equipment and the ability to deploy that in a severe emergency.

Mr. WALDEN. By the way, a side question—do you involve the amateur radio community in your emergency drills at all? I confess, I am one. But it also is a very dispersed—it's like the original internet, right?

Mr. CAULEY. We have not particularly sought after that, but I know Dr. Beck and his crew at EIS has had some work around the use of ham operators for emergencies.

Mr. WALDEN. Yes, they are the only communication tool left. But go ahead, Mr. Aaronson.

Mr. AARONSON. So a philosophical question but I won't give a philosophical answer. I think the culture issue around, and you alluded to it, that people are very much tethered to their devices and very much reliant on this.

We have found, even in storms, while the industry has gotten considerably better at restoring more quickly, if you do a good job of preparing the general public ahead of time power will be out for a short period of time. This is what's going on to restore it, I think helping people understand that it may not just be storms anymore but there are other sorts of threats whether cyber or physical or otherwise that may have an impact, and if they can be prepared and they understand that we are preparing I do think there is a really important public policy and public communication role that the Congress and federal policy makers in general can play.

I'd also say just from cultural perspective, there has been this tendency to blame the victim when incidents do happen on critical infrastructure operators. Look at Sony, look at Target.

Changing that dynamic a little bit so that people recognize when you're talking about very sophisticated threat actors and near pure nation states who are targeting critical infrastructure, and I think, again, if people recognize there is a partnership between industry and government, that we are working on this, that we are heartening our systems, that we are more resilient, I think that can go a long way.

One last quick note, I would say this, and you alluded to it a bit, this reliance on a culture of compliance. Security can never be a

check the box exercise, "OK, I've done X, Y, and Z and therefore I am secure."

No. Actually, it's the opposite. You are complacent and, again, going back to culture, I think helping people understand that this is a journey without a destination, but it is one that we are all on, will help to prepare your constituents, our customers, for the new world that we live in.

Dr. BECK. I would say, going to Scott's point about the social aspect, to your question, Chairman Walden, that I don't see any regulation currently that's hamstrung the efforts, but they are challenged by two social structures: stovepipes and tunnels.

Stovepipes we are more familiar with and those have to do with, for example, government agencies that can be one stovepipe or infrastructure sectors that we need to work on getting more discussion through those stovepipes or those silos.

But the other one is tunnels, and what I mean by that is there is communication and common understanding at specific levels of decision making. So CEOs understand each other and they have a certain view of a situation.

The engineers that work on cybersecurity have a different understanding of it. The CFOs, et cetera, and so we need to look at all of those, breaking down basically both silos and tunnels so that there is a common operating picture and mission.

Ms. SUGG. There has been a lot of comments here that I could echo and I'll save the time on that. Innovation is important. Working together through the ISACs, through multi-disciplined ISACs are important.

Continuing to work closely with the Edison Institute. Their work is phenomenal and is benefitting the entire industry. And through NERC to evaluate what's coming out of the government and how do we best prepare ourselves within the framework.

I agree about it's important not to vilify the company that does indeed get breached because we will all learn from it. Someone else's detection is everyone else's prevention. So thank you.

Mr. UPTON. Mr. McNerney.

Mr. MCNERNEY. Well, I thank the chairman and I am going to follow up on one of your questions with Mr. Aaronson.

Do you think that transformer standards would help reduce the threat of transformer attack or do we need a strategic reserve of some kind?

Mr. AARONSON. So I think as you know the electric grid grew up in fits and starts over, quite literally, the better part of a century and as a result there are these different voltage classes and sort of a mishmash of equipment across the sector.

Interestingly, that's not necessarily a bad thing. It does create some biodiversity, which in and of itself is a protection mechanism.

So I think standardization within reason may be something worth at least exploring. With respect to a strategic reserve, I think this is one of those instances where government and industry have to be aligned.

Industry, as I mentioned, has the Spare Transformer Equipment Program, has SpareConnect, has Grid Assurance, has Restore, has these other bilateral arrangements and multilateral arrangements across the sector.

Those are really useful and have grown up out of necessity and have been utilized. To the extent that there are opportunities for the federal government to provide additional backstop, additional spare equipment, not just limited transformers but are many other critical components and support for moving them. Filling the gaps that the industry observes, I think that's a useful pursuit.

Mr. MCNERNEY. Thank you.

Mr. Cauley, do you feel that the trend toward distributed generation makes our electric system less or more vulnerable to cyber-attacks?

Mr. CAULEY. Well, it's a great challenge and a great dilemma that we face in front of us. In some respects it creates a system that's more resilient because there is more resources and capabilities that are more distributed, and there are greater redundancies in the system and I think it enhances reliability and resilience.

The challenge is that all those devices are going to be communicating with something else and in some cases they are much closer to the internet than the bulk power grid.

So it's going to create a much greater surface to attack and can create multipliers in the attack where you have common devices that are out there. Instead of there being three breakers of a certain model, there are 1.5 million devices that are exactly the same and can be simultaneously hacked.

So it goes both ways and I am deeply concerned that we continue to focus on the distribution side in terms of getting security right and getting it built into those systems.

Mr. MCNERNEY. Thank you.

Ms. Sugg, how effective would cyber hygiene, education, and enforcement be in preventing successful cyber-attacks?

Ms. SUGG. Cyber education is extremely important. Security awareness is important. We cover everything in our training and education from how to ensure that you don't click on e-mails on to how to recognize an event within the systems at any given time using some of our advanced security monitoring.

That awareness is required as part of the standards, which I think is a very healthy requirement for us. But we don't just limit that to the people that work within the scope of the critical infrastructure.

We expand that awareness and education to all of our employees, recognizing that each of them has an opportunity and a responsibility to help us protect all of our systems.

Mr. MCNERNEY. Thank you.

Mr. Beck, with the internet of things are there concerns about potential cyber threats from systems that are already in place but we haven't seen incidents yet?

Dr. BECK. Certainly, the question is the continued expansion of the internet of things or even going back to your question of Mr. Cauley about distributed generation.

As things are introduced and connected into the grid, what is an important practice is, if we are going to try to stay ahead of the threat, to have it be a part of design philosophy when new devices or processes are put in place.

We don't want to connect things and then say oh, gosh, we forgot about cybersecurity—now we have got to do a bunch of patches and

things. Again, it's more of a social issue of trying to get security practices baked in to new development as we go forward, and we can grow your way to greater security because the grid is always expanding, things are always being updated and replaced by new equipment, better processes and so on. And if that new equipment and better process includes security as a baseline feature of its design and implementation, we will be safer.

Mr. MCNERNEY. Well, I've been involved in standards committees and I know how slow and deliberate they are. Are standards able to keep up with the threat in terms—even actually the definition of what cybersecurity and threats mean?

Mr. CAULEY. Well, I think they certainly help provide a baseline even as the topic was just about distributed systems and internet of things.

IEEE and other technical equipment standard-setting organizations could have standards built in to make those devices more equipment. The tendency to selling to consumers is to make them as easy as possible to plug in and set up, and that really creates a difficulty.

So I think there is room for standards to set the baseline in terms of how protected individual equipment should be.

Mr. AARONSON. If I could just piggyback on that. I think the answer is yes, but standards have a role.

They cannot completely keep up with a very dynamic threat, and I wanted to just weigh in really quickly on the question about distributed resources.

I think Mr. Cauley hit it on the head. It's sort of a paradox. There is some resilience that can be brought from distributed resources, but it broadened the attack surface and, largely, these are consumer-grade electronic devices that do not have the same security standards, to bring it back to that question that may be necessary.

Another challenge is visibility from the operators of the grid into these distributed resources. It's a misnomer to think these distributed resources are not connected to the grid.

In fact, they have to be. Having a rooftop solar panel if it's not connected to the grid is like having a computer not connected to the internet. You need to be a part of that broader ecosystem.

So ensuring that there is security baked in, not bolted on to those pieces, and that the owners-operators have visibility into the power that's being generated is going to be critical to ensure reliability and resilience for the rest of the sector.

Mr. MCNERNEY. Thank you.

Mr. Chairman, I yield.

Mr. OLSON. Gentleman's time is expired.

The chair calls upon the Vice Chairman of the full committee, Mr. Barton from Texas, for 5 minutes.

Mr. BARTON. Thank you, Mr. Chairman, and I apologize for not being here at the beginning.

I had, as some of the others, the hearing on the Medicaid program in the Health Subcommittee downstairs. So I am honored to be a part of this subcommittee also.

I want to recognize former Congressman Ross out in the audience, a valuable member of this committee in the past, and I think

probably the subcommittee, and you're looking very happy being a former member. So we are glad to have you.

The purpose of the hearing today, Mr. Chairman, as you well know, is to discuss what we are doing and look at trying to protect our electrical grid from the threat of cybersecurity problems.

We have the president of the organization responsible for protecting us, Mr. Cauley. So I am going to ask the other three witnesses, Mr. Aaronson, Dr. Beck and Ms. Sugg.

Ms. Sugg, what kind of a job do you think he's doing. Is he doing a good job? A bad job? What do we need to do to encourage him?

Mr. AARONSON. And I am not saying this just because he is sitting right next to me, but I think he's doing an extraordinary job and I think that the North American Electrical Reliability Corporation serves an exceedingly important role as the electrical reliability organization as directed by this committee and Congress through the Federal Power Act.

It is a challenge to be sure, but I do think the role that they play between a regulatory body that is pushing standards and, regulators regulate—that's their responsibility. But also then to organize the industry and ensure that the engineers and grid operators have a voice in the standards that have to be developed for reliability of the system to make sure that these standards: number one, keep up with technology; number two, are flexible enough, as Ms. Sugg referenced, and that they can apply to the smallest of the utilities—and the largest investor-owned utilities in the nation is a challenge but one that I think Gerry can pass.

Mr. BARTON. You give him an A?

Mr. AARONSON. I'll give him an A.

Mr. BARTON. Dr. Beck.

Dr. BECK. I'll second that, and I want to say that I appreciate that Mr. Cauley has been a support for EIS Council and that we have appreciated the fact that we have been able to have discussions with NERC regarding our shared areas of interest and he certainly didn't have to do that.

But we discovered that focusing on what we consider outside, and beyond just the professional realm of regulating the electric reliability, is fundamentally we are all interested in the security of our families and our fellow citizens and the nation as a whole, and I think that our shared commitment in that has allowed us to work together to share ideas and we appreciate that partnership.

Mr. BARTON. OK. Ms. Sugg.

Ms. SUGG. We appreciate the partnership with NERC as well. Our experience is that NERC is very collaborative. They listen. They ask a lot of questions.

They hold us accountable for standards but more so, and I've heard Mr. Cauley mention this numerous times in other arenas, that it's more important to focus on security and to shift that focus from just being focused on or worried about being compliant to being secure.

The standards drafting teams that are led by NERC that pull together industry experts to develop the standards, to really understand how best to put a standard in place that doesn't become overly restrictive, is very healthy for the industry.

And I also find that NERC is receptive to understanding or hearing additional conversation about standards that do exist that are already in place. Not just standards that need to be developed, but to understand the challenges that we have with them and ensure that they stay as robust as possible without limiting us in our technologies. I give him an A.

Mr. BARTON. It's very rare that Congress does something that, this system came from the Energy Policy Act of 2005, which I was chairman of the committee and the chairman of the conference committee. So I guess I'll pat myself on the back.

But I am going to give you the final word, Mr. Cauley. You've just gotten three As. That's a pretty good report card.

Is there something legislatively this subcommittee and full committee needs to do to improve what appears to be working or are you happy with the authority you have and just want to be left alone?

Mr. CAULEY. I appreciate the question and the previous question and the responses.

Mr. BARTON. They expect you to take them to dinner tonight because of their answers.

Mr. CAULEY. Something along those lines. I think the testament to the legislation creating this framework that our data, not our view but our data that we collect from industry, is that reliability of the bulk power system has improved over the last 10 years and that's the testament that we want to leave is that we are getting better on the bulk power system in terms of number of outages, frequency of outages, impact on customers.

I think the framework works. Our relationship with FERC is excellent and when we have got to get something really important done, like they said, let's do a physical security standard or a standard on GMD. We have a conversation. They direct us to do it and we do it and we meet their requirements.

The one area where I think we continue, particularly in the area of security, or we need to continue to work on is the ability to share information between industry, NERC and the government, and sometimes we do it well and sometimes we don't do it well.

There is always the challenge of what's classified, what's secret, what's sensitive to the military. But we crave information in industry to figure out what we need to do to protect the grid and to get that free flow of information. To have it be protected is essential for us. Thank you.

Mr. BARTON. OK. Well, downstairs we are fighting like cats and dogs. But in this subcommittee on this issue we are hugging each other.

I think we can work together if we need to and I want to thank the witnesses and thank the subcommittee vice chairman and the subcommittee ranking member for holding this hearing.

Mr. UPTON. The gentleman's time has expired.

The chair calls upon the gentleman from California, Mr. Peters, for 5 minutes.

Mr. PETERS. Thank you, Mr. Chairman. Thank you to the witnesses for being here.

So in 2003, my wife and I took my two kids to New York. We thought we'd get some good food, visit some friends, see "The Lion

King" and we, of course, were there for the blackout. So we had a nice Italian meal the first night. The next night was salami and crackers and still never seeing "The Lion King."

But the impressive thing about that was that it all came from some glitch in Ohio. So I guess we are inferring from your comments about the reliability of bulk power that that sort of thing has been improved upon.

But it did also make me think about distributed generation because one of the things that we have seen in San Diego in the defense sector is a development of micro grids.

At Pendleton you see this all over, and it seems to me that for redundancy and reliability that offers some advantages. But I had the same question about the portals into the system for attackers.

And you've sort of answered the question but Mr. Aaronson said something that I want to follow up on, which was you want security baked in to these devices, not bolted on.

What can we do from this subcommittee to make sure that that happens?

Mr. AARONSON. So let me refer to the '03 blackout for a second, also. While that was not the best day in the history of the electric utility industry, and I think Ms. Sugg hit it on the head that someone's detection is someone else's protection.

We learn from all of these experiences and in fact Congress learned from that experience and in its wisdom, as Mr. Barton was referring to. The Energy Policy Act gave way to the ERO and here we are.

I think there is something to that, which is observing where these gaps in security may lie with distributed resources and ensuring that if they are going to be a part of the bulk electric system that they have a certain level of security that they are responsible for as well.

Again, as owners/operators, who have bulk electrical system responsibilities, I think those who might be able to impact the bulk electric system should share in that responsibility.

Again, it goes to my point about visibility, also. One of the things that was learned after '03, it was a cascading blackout, but the system worked precisely the way it is supposed to. The system failed safe.

Now, that doesn't change the fact that you haven't had a chance to see "The Lion King" but it does show that cascaded from Ohio up through Quebec into the northeast, stopped in New York, didn't go down the entire Eastern seaboard. Spinning equipment was not damaged and we were able to restore power within a reasonable amount of time, 48 to 72 hours.

Again, not the best moment in the utility industry's history, but a show of how resilient the system is in fact. I want to make sure to maintain that resilience and don't want to lose visibility or resilience because of a rapid proliferation of DER.

Mr. PETERS. Talk about the distributor or the stuff that's outside the bulk power system. So, maybe a military micro grid has better protections than the average household device.

But I am thinking, now you have these home devices. You turn energy on and off. I assume that that is a point of vulnerability and what do we do to make sure that the security you talked about is,

as you said, baked in? What is it that we need to do? Is it standards or what would it be?

Mr. AARONSON. I think it is standards and requirements. We talked earlier about the internet of things, and these are your devices like a thermostat, like a refrigerator, like a baby monitor, that are being put out at—I think about five and a half million per day and by 2020 we are going to have something like 20 billion of them connected to the internet.

And these things have hardwired passwords that are default passwords. These things are easy to break, and if we are talking about things that have any relationship to critical infrastructure I think having that low a bar of security, that consumer-grade electronics tend to have, is a concern for us in the industry.

Dr. BECK. I would just add that, again, putting the baseline standards is necessary but it also needs to be customer driven.

Customers need to say I am not going to buy a device that has hardwired passwords that I can't change and it's just the name of the company or the device.

Mr. PETERS. On the other hand, just take it at the most basic level. Take someone who's putting solar on their roof. They may not care. Why would they care about the larger grid? What is going to be incentive for an individual customer to talk about that?

Dr. BECK. Well, I think, again, it's trying to make everyone aware that when you're this connected then your vulnerability becomes someone else's problem, not just your own, right.

So you can have negative impacts on your neighbors' other systems if you don't care. So we have to get, again, people to care about this in a broad sense.

Mr. PETERS. All right. Well, I'll look forward to working with that. My time is expired. Appreciate it. Thank you, Mr. Chairman.

Mr. OLSON. Gentleman yields back.

The chair calls upon himself for 5 minutes and welcome to our four witnesses. As a congressman from the state that consumes the most energy in America, Texas, cyber-attacks on our electric grid have caused me to lose sleep on occasion.

We all know about Russia's attack on Ukraine in December of 2015. That was kind of easy. They have e-mails of employees are standard format, first name dot last name dot organization dot com, dot org, something like that.

Got those, put attachments on those. Sent them back. Opened up, they deploy and they shut down some circuit breakers.

As has happened charged said the response was all they could do was film the attack with cell phones. Film the attack with cell phones.

Now, I know that we're not like Ukraine. We are much more advanced. But in the Navy, I was a pilot for 9 years. They teach us to prepare for the worst, hope for the best.

And so, Mr. Aaronson, along those lines, hypothetically, if the lights go out all over D.C. as this hearing ends—we are attacked, a cyber-attack—what chain of events does that start like that?

Mr. AARONSON. So that has happened before and in fact not long ago there was a voltage dip that occurred because of a fire at a substation and the lights, in fact in D.C., did go out. And in that first

hour it was unclear why. We knew about some incidents around the greater metro area. But was it terrorism?

This idea of fog of war in the midst of an outage, was it something typical like a voltage dip and those things happen? Was it an act of terrorism? Was it cyber? Was it physical?

Getting ground truth on that is hard and attribution is hard. But having the mechanisms in place to talk to each other is important.

So in that instance, and if there were something Ukraine-like to happen here in the U.S., it's less about why the power went out and more about simply restoring at that moment.

Ukraine was a great example, as are all of these incidents that happen all over the world and here domestically, to get us better at resilience and the idea is to take the lessons learned, apply them and get better.

In the instance of your hypothetical, what would happen is there would be an immediate high level of coordination between the ESCC and CEOs in the industry along with senior government officials and including Mr. Cauley and his team from the Electricity Information Sharing Analysis Center.

In the case of the voltage dip a few years back, that also resulted in a phone call with DHS on something known as the NICCL, the National Incident Communications Coordination Line, and that NICCL call actually had folks from both the affected utility and DHS and White House leadership.

And what it allowed us to do was have White House leadership, at the time Josh Earnest was the White House press secretary, go to the podium from the most important podium in the land and say this was not a terrorist attack. We knew what was going on.

So that really tight coordination between senior government officials and the industry proved itself to be just invaluable.

Mr. OLSON. To recover how do you share those lessons learned with government and industry to make sure that we learn lessons from these attacks through incidents because that's an important part of the whole process.

We are attacked. Whatever happens learn from it. So how, Mr. Aaronson, how do we share that with industry, with the federal government?Mr. AARONSON. Those mechanisms exist and they are getting better all the time. I am particularly proud, again, as part of the secretariat for the Electricity Subsector Coordinating Council, the ESCC is a place where that happens.

But, again, the E–ISAC and Gerry's organization play a significant role. The sector as a whole, we operate one big machine with thousands of owners and operators. There is this shared responsibility. So when a thing happens we are particularly good at coming together, applying those lessons and making sure that in the future a similar incident would have either less impact or no impact at all.

Mr. OLSON. Mr. Cauley, do you have an answer about recovery?

Mr. CAULEY. Usually what we are doing is as quick as possible situation assessment, put the system back together. If we have damaged equipment or computers, we will isolate those and start putting the system back together as quickly as possible.

Why reliability has gotten better the last 10 years is because we are always learning from every single event, small, medium, and large, and we get the information out to industry.

Mr. OLSON. Good. Dr. Beck, add anything to those line of questioning?

Dr. BECK. I think there is challenge in learning lessons and protection of the herd because there is a natural tension between restoration and attribution.

So to do attribution sort of like any crime scene, you don't disturb the scene. You rope it off and then you analyze it and try to figure out what happened, but that crime scene is a broken down system that the operators want to restore.

They don't want to leave a mess that people can look through. It's just a challenge. Nobody's wrong. Both things are important, but coordinating on attribution could be important certainly for a very sophisticated attack that may be distributed and that we don't know where all it is embedded.

Mr. OLSON. Ms. Sugg, anything to add from your perspective, ma'am?

Ms. SUGG. From the ISO/RTO perspective, certainly we are going to work closely with NERC and support the information-sharing opportunities that exist to learn from these events.

In the midst of that crisis, our operators are going to be looking for what's going on in a particular area of the footprint. I believe Washington, D.C. is in the PJM footprint.

And so PJM operators are going to be looking for ways to contain a particular system outage to keep it from having broader cascading effects across their region. That's just one of the responsibilities of reliability coordination within the ISO/RTO community.

Mr. OLSON. Well, thank you. I'll sleep better tonight, I guarantee you.

One final question—you might know the incoming Secretary of Energy is a guy from Texas, Governor Rick Perry. He's a friend, and Governor Perry asked me to ask of you all, in his new role over at Energy what is the one thing he can do, one thing, to help you make our grid more secure, from DOE's perspective? Your perspective on DOE?

Mr. AARONSON. I'll say it again. ESCC, working as closely as possible with industry leadership, we have enjoyed a very fruitful relationship with the Department of Energy because of their senior leadership being committed to it and we look forward to and know that Secretary Perry will continue that tradition.

Mr. OLSON. Anything else to add, Mr. Cauley?

Mr. CAULEY. I will echo that. Just to get engaged with the industry leadership. We have several meetings a year with high-level folks from DOE, DHS and others, and we engage them in our exercise.

We challenge them and make them uncomfortable, but we have grown together in the last couple years and I think with the change of administration we need to renew that.

Mr. OLSON. Yes, sir. Dr. Beck, anything to add on that, sir?

Dr. BECK. I would say, commensurate with the incoming administration's emphasis on infrastructure that leadership be shown there, and to pay attention to the electric and fuel infrastructure

that supports it and, again, to ensure that security is part and parcel also with efficiency and reliability so that they are on equal footing and that those practices are embedded in any new infrastructure.

Our infrastructure should always be getting more secure as it is upgraded. We can't be introducing or reintroducing old vulnerabilities or introducing new ones.

Mr. OLSON. Ms. Sugg, your comments.

Ms. SUGG. I would encourage continued collaboration across the various industries that are dependent upon each other and I would also encourage the DOE to continue to focus on developing their cybersecurity frameworks that are made available to utilities to help ensure that we are thinking about security from soup to nuts and not just focused on the current threat or the current issue on the front page of the paper.

Mr. OLSON. Well, thank you all. On behalf of Governor Perry, much obliged.

And my time is expired. I now recognize the gentleman from Pennsylvania, Mr. Doyle, for 5 minutes. He has departed, so I guess it's going to be Ms. Castor from Florida for 5 minutes.

Ms. CASTOR. Thank you, Mr. Chairman.

Good morning and thank you for being here today. Mr. Cauley, to date the power grid in the United States has not lost any service hours due to a cyber-attack, correct?

Mr. CAULEY. Yes, ma'am. That is correct.

Ms. CASTOR. OK. Nevertheless, the electricity sector has not been invulnerable to cyber-attacks. As recently as December a utility in Riverside, California experienced a cyber event that did not cause a blackout but potentially could have affected grid reliability, according to an account on file at the Department of Energy.

The same month, suspicious activity was detected on laptop at a Vermont electric utility, which was not connected to the grid.

Does NERC have data on cyber-attacks against utilities that have not resulted in a loss of power on the grid?

Mr. CAULEY. Yes, ma'am. We track pretty much every incident and they are as small as incidents around a compromised laptop, which both of these cases were.

They are connected to the corporate systems and the business systems of the enterprise and not to the electrical controls of the grid, and both of these were reported to us through our regular reporting capability.

We understood what they were. Basically, the corporate side of each utility is as exposed to the outside world as any other business and you have to have that diligence around that and we are also subject to human frailties, people going onto a particular site so the idea is to continuously monitor, catch those and fix those. But both of those organizations reported to us.

They did the right thing and we were able to distribute that information to the rest of the industry so that they could look for the same kind of issue.

Ms. CASTOR. I think you're right. Oftentimes the weakest components in security are the humans that have to interface with the systems. Spear-phishing attacks have resulted in major leaks when even savvy users relinquish their passwords.

And everyone is very concerned about what happened in the Ukraine and I—this was a good little article by security writer Kim Zetter.

Everything we know about Ukraine's power plant hack—that the end of December two power distribution companies in Ukraine said that hackers had hijacked their systems to cut power to more than 80,000 people.

The intruders also sabotaged operator work stations on their way out the digital door to make it harder to restore electricity to customers.

The lights came back on in three hours in most cases but the hackers had sabotaged management systems and workers had to travel to substations to manually close breakers that hackers had remotely opened.

And days after the outage Ukrainian officials appeared to blame Russians for the attack, saying that Ukraine's intelligence service had detected and prevented an intrusion attempt by Russian special services against Ukraine's energy infrastructure.

Speaking at the S4 security conference, former NSA and CIA spy chief General Michael Hayden warned that the attacks were a harbinger of things to come for the U.S. and that Russia and North Korea were two of the most likely culprits if the U.S. power grid were ever hit.

Now, what was interesting is utility operators in the Ukraine began experiencing small attacks 6 months prior to the main attack.

These included e-mails to utility operators containing documents which installed malware. Could spear-phishing attacks and other similar intrusions represent a vulnerability to grid systems if hackers are able to identify information about grid systems by first infiltrating the personal and business information of the grid operators and what are we doing about that?

Mr. CAULEY. Well, spear-phishing, going to malicious sites, picking up malware on a laptop or a computer is probably the greatest vulnerability that we have and the most challenging to manage.

I am pretty sure that the situation in the Ukraine would not happen here, because they failed to really recognize between March of 2015 and December 2015 we would not allow that software to go unchecked and for the perpetrators to get elevated credentials so they could actually operate the system.

Those are extreme violations of all our rules and all our checks and balances and the controls that we have in place. I don't view what failed there is that an operator clicked on the wrong link.

I feel that the organizational and institutional framework failed to have the rules in place to make sure that those are constantly checked. Humans will make mistakes.

It should not last on a laptop more than hours or days before they get detected and fixed. It takes months to perpetrate a campaign like that, and it did in this case. But you got to use that time to figure out you've been compromised and fix it.

Ms. CASTOR. I appreciate that and I appreciate how all of you today have expressed sincere understanding all of the security facets of this.

But please be cognizant that a lot of this can start with those innocuous looking smaller type of infiltrations and I hope that you're talking with all of your personnel about that, too.

I trust that you are. Thank you very much.

Mr. OLSON. The gentlelady's time has expired.

The chair calls upon the gentleman from Pennsylvania, Mr. Murphy, for 5 minutes.

Mr. MURPHY. Thank you, Mr. Chairman, and thank you to the panel, too.

First of all, I want to make sure we know in the record as far as the Ukraine goes—a bigger threat to their grid is the fact that Russia has invaded them and Russia has taken their coal fields away and that Russia threatens every European nation that is under the boot of Gazprom and that's what they do and they say if you don't buy our gas from us and you don't do this we are shutting off the pipes.

So that's a big concern, too. But doing it through a back door avenue of a cyber-attack is important, something we all should pay attention to and I hope that our new president establishes good negotiations with President Putin so we can get back to the work of doing other things.

But I wanted to ask about another area here. When it comes to working with the cyber-attacks and prevention, et cetera, we know that—I think it was Home Depot was hacked and they were hacked because they went through some small level billing—an HVAC system that didn't have the kind of protections. They worked their way through those channels to finally get into their——

Dr. BECK. That was Target.

Mr. MURPHY. Oh, it was Target? OK. May have been they find some little area that doesn't have strong defenses here. And so I am wondering also in the utility sector and the power grid sector what can the federal government do to help to enhance cybersecurity, noting that someone may come in through any door, any unprotected door in this.

Does anybody have any ideas of how this could be? Any supplier to a power plant, any supplier that they could find some weak link there? Mr. Aaronson, do you have a thought on that?

Mr. AARONSON. So a couple of observations, and it brings in Ms. Castor's point about humans also. The weakest links, whether it is an unsavvy vendor, whether it is even a savvy user, there is always the joke.

There is hardware vulnerabilities, there is software vulnerabilities and there is wetware vulnerabilities, and we are the wetware.

I think, going back to my original testimony, as owners and operators we have to be right 100 percent of the time and the adversary has to be right once, I think looking at the weakest link shows that there are a lot of opportunities for the adversary to be right.

But them being right does not have to be catastrophic. It goes to this idea that Mr. Cauley was talking about of the cyber kill chain.

Seeing early precursors to potentially more nefarious or destructive activity, predictive analytics that help us to see those and

being more aggressive in that cyber kill chain to both prepare, protect, and defend but then also being able to respond and recover.

And to bring this back to Ukraine, while I agree with Mr. Cauley that a similar attack in the United States is very unlikely, but not impossible, I do think that the lesson that we have learned from them is they were able to get their 200,000-plus customers back up and running within about 6 hours. They were operating in a degraded state but electricity was still flowing.

Mr. MURPHY. Thank you. So let me ask this, though, because with regard to the grid, do any of the larger customers have any kind of other software and other controls that can pull off the grid and demand more?

So if there was, obviously, not control of the power plant, but do they have any kind of links than can affect if they are not getting enough?

Do all those controls have to go back through the original utility company and the power company on that grid if they experience some problems?

Mr. CAULEY. I think the general answer is that the system is built to be very redundant and with excess capacity. So if something is damaged or not behaving correctly it can be removed and there is plenty of capacity to move energy around.

Mr. MURPHY. Sure. I am wondering about the two-way communication. I am also looking for other back doors in there, too.

Two of the things that we have in Pittsburgh—one is the Carnegie Mellon University computer emergency response—the global leader in this and also there's another program there called the National Cyber Forensic Training Alliance, which is a room filled with lots of cubicles of businesses of every shape and form, and when one picks up something they announce it. It's like the stock exchange.

Someone says hey, I've got something here and they start looking back and forth and see where these back doors—channels are starting to probe—where's the Trojan horse running, et cetera.

And I am wondering that it's one of the areas the federal government can look at because sometimes we will silo these off—let's work on DoD, Navy's going to do their thing, Army's going to do their thing, Air Force is going to do their thing, Commerce is going to do their thing, maybe different parts of Energy.

I am wondering do we have enough cooperation between different branches of the federal government and working at these things together so are we creating more inefficiencies in our system.

Dr. Beck, go ahead.

Dr. BECK. Well, it's still a challenge. So I talked about the silos before. But I would say no but it is improving. The information sharing needs to be done with regard to sharing research, with regard to what are the problems you're trying to solve.

Mr. MURPHY. This may be part of the lesson to take back to the new secretary of energy, that people have to be willing to play together in the same sandbox and share their toys.

Dr. BECK. Right. So you have DOE labs and you have DoD labs and they don't talk to each other very much, but they could with leadership and they end up working on similar problems and find out later wow, we have a military application. We had a problem

here but 90 percent of that problem might be relevant for a civilian electric power grid.

It takes the ability to share information at least at a high level and then be able to dig in and share that possibly if it's classified but at a more technical level as well.

Mr. MURPHY. Thank you. I appreciate that. I yield back, Mr. Chairman.

Mr. OLSON. Gentleman's time has expired. The chair calls upon the gentleman from New York, Mr. Tonko, for 5 minutes.

Mr. TONKO. Thank you, Mr. Chair.

Welcome to our panelists. This subcommittee heard from Secretary Moniz about the interdependence of our critical infrastructure.

And from what we heard this morning, it sounds like there is agreement that the security of our grid infrastructure is particularly important because of so many other sectors relying upon it. Is that a fair assessment?

Mr. CAULEY. Yes, sir, and we drive that out when we do our exercise and we break everything down. Financial sector, transportation, telecommunications, water—we are as dependent on them as they are on us.

Mr. TONKO. OK. Thank you. And while I appreciate the focus on increasing security and mitigating cyber risks, I am also interested in knowing more about procedures in case there is a major cyberattack.

So, thankfully, our country has not had any major cyber incidents that have needed response but we have had major natural disasters. I would cite as an example in my home state of New York we dealt with Superstorm Sandy in 2012.

What specific lessons have been learned from the response to major natural disasters that may be applicable to a future cyber-related response effort?

Mr. AARONSON. So I think it's fair to say that the lessons in coordination, because we have not had an opportunity outside of exercises to necessarily exercise and stretch those muscles with respect to a cyber incident. They have grown up with respect to natural disasters and a couple physical security incidents as well.

That partnership is invaluable. I look at the role that the Electricity Information Sharing Analysis Center plays. I look at the role that the Sector Coordinating Council plays in coordinating with the highest levels of the industry.

I look at our partnership with DOE, who operates under emergency support function 12. Not only are they our sector-specific agency, but they are the electric sector's entre into the rest of the federal government enterprise, working closely with DHS, working closely with FEMA, working closely with the Department of Defense.

A great example was Superstorm Sandy, when we did have the opportunity not just to help inform but actually be in the interagency room and help to direct resources where they needed to be directed. So taking information from affected utilities and feeding it into the government and taking information from the government and feeding it back to affected utilities, that same battle rhythm would be seen in the event of a cyber incident as well.

Mr. TONKO. So the intercommunication is important and I see you all kind of nodding in regard to that. So do you feel the procedures, the equipment, the personnel are in place in order to respond to a major cyber incident today?

Mr. AARONSON. I think the proper answer is it depends. That's always the proper answer. No, I mean, to give some modicum of comfort, yes. I think these relationships and these processes and these exercises have really informed and these experiences have really informed the industry's not just security posture, but response posture.

I do think there is the added complication with cyber of data assurance, knowing that the data you are reacting to is the right information or has not been compromised in some way. So we are very cognizant of those challenges.

But I do think just simply having that underlying foundation of partnership and response capabilities makes us fairly well prepared and getting better all the time. That's the goal.

Mr. TONKO. OK. Dr. Beck, did you want to say something?

Dr. BECK. I would say I largely agree with that but, again, with particular respect to cybersecurity, there are additional challenges to expanding mutual assistance, which the industry has a long history of.

When it's a physical system—your example of Superstorm Sandy, those were mostly downed poles and lines. The equipment was standard. The repair techniques and knowledge was standard.

Within any utility's OT system you're going to see more variation than you are between poles and lines. And couple that with Mr. Rush's point earlier about a smaller cyber workforce. It's a resource challenge. I applaud ESCC for taking it up.

But it is more challenging than traditional mutual assistance.

Mr. TONKO. Let me just quickly get this in. You all partner with the Departments of Energy and Homeland Security and, obviously, they provide a lot of expertise.

But can you discuss your relationship with state and local governments? And I would just throw the caveat out of New York, again, working to develop their own cybersecurity capabilities. They've done this with the National Guard.

Both New York and New Jersey National Guards have created a partnership to form a cyber protection team. Just your response to that, please.

Mr. AARONSON. So I was remiss in not mentioning, as Dr. Beck did, the cyber mutual assistance program and agree completely with his assessment that it is in its nascent stages and mutual assistance in its traditional form was born under the crucible of lots and lots of incidents of natural disasters over the years.

The same will be true of cyber, and to bring it to your question about state and local, a state chief information officer once said to me states are the consequence people. And you certainly see experiences where governors and the local, national, and the state National Guard work very closely with their utilities.

Those partnerships are in place. The cyber mutual assistance program is leveraging those relationships for two reasons: one, states are the consequence people; two, the National Guard has some extraordinary capabilities that can help augment and com-

plement and supplement the capabilities that the industry brings to bear with its cyber mutual assistance program.

So I would say working closely with governors at the highest level, I would say working with operators and helping to bolster the cyber mutual assistance program with the Guard and then I would say sharing information at the local level through fusion centers.

And, again, there are 73 fusion centers across the country. The joke has always been if you've seen one fusion center you've seen one fusion center, but they are increasingly better at coordinating amongst each other at the state level and giving us yet one more tool to share information and better respond in the event of an incident.

Mr. TONKO. Thank you very much. I yield back, Mr. Chair.

Mr. OLSON. Gentleman's time has expired. The chair calls upon the gentleman from Mississippi, Mr. Harper, for 5 minutes.

Mr. HARPER. Thank you, Mr. Chairman, and thanks to each of you for being here. This is such an important topic as we go forward so I appreciate all the input each of you have given.

Mr. Cauley, if I may ask you a couple of questions here. Is the North American Electric Reliability Corporation's alert system working as intended to provide the concise actionable security information to the electric industry?

Mr. CAULEY. Yes, sir, it is, and we are able to get out information very quickly if needed, within an hour if needed, and it gets to all of the owners and operators of the system with the specific information and they have access to it directly.

So we are always looking to make it better. I think in the Ukraine and the internet of things incident that we saw in the last 12 months we have learned to scale.

We can get thousands of people now on a conference call and let them know immediately what's going on, including the CEOs and others.

Mr. HARPER. What are the threats outside the bulk power system?

Mr. CAULEY. The threats to the grid outside the bulk power system?

Mr. HARPER. Yes.

Mr. CAULEY. Well, I think we touched on it earlier. There are much more electronic digital devices that exist in the distribution system and then customer systems that I think are going to increasingly have an influence on the overall grid.

Mr. HARPER. Let me just follow up just a little bit. As you previously stated, the North American Electric Reliability Corporation uses an alert system to notify the electricity industry of the issues or problems.

You note that North American Electric Reliability Corporation determines the appropriate alert notification based on the risk to the bulk power system. How do you determine the risk or the level of that risk?

Mr. CAULEY. We have expert folks on both the cyber side as well as the operational side of the grid to know what the potential impacts might be and this is actually one of the particular values that we add in our relationship with Department of Energy, DHS, and

the FBI is they often ask us what does this mean and how would it affect the grid if it actually happened.

So we have both sides of that expertise and we have people who work in classified space to interpret what it means and what the potential downside could be if this actually happened.

Mr. HARPER. OK. Obviously, other business sectors depend upon electricity. We have discussed that. But can you explain how the electric sector is dependent and reliant on other sectors and what is the industry doing to reach out and address these interdependencies for better cybersecurity?

Mr. CAULEY. Well, we are reaching out to the other sectors. I think the dominant one is the telecommunications industry because a lot of our control systems, the ones I mentioned earlier, were so essential that we want to protect the most run over communications networks.

The majority of those are privately owned by us through services with some of the major vendors. But if those systems go down, and you look at the example of Hurricane Sandy when some of the major telecommunication suppliers had vaults in buildings in Manhattan that were flooded with water, we depended very much on those communications capabilities.

Water, transportation—finance is one you might not think about but if there is a severe enough event utilities need the liquidity to get everything done and recover and pay their folks and pay for the emergency housing and things like that.

So there are a lot of dependencies that we are working on through the expanded relationship that Mr. Aaronson had talked about of getting the same level of CEO support that we have in the electricity industry.

We want to get with those other sectors and get them all in the room with the government folks that we need to work with to make sure we are communicating and coordinating and planning together.

Mr. HARPER. Well, I want to commend each of you on the level of cooperation and communication that you share and appreciate the effort that you're making.

Thank you. I yield back.

Mr. OLSON. The gentleman from Maryland, Mr. Sarbanes, for 5 minutes.

Mr. SARBANES. Thank you, Mr. Chairman. I want to thank the panel.

I am trying to get my head around how much of these efforts to protect the grid from cyber threats and so forth is an exercise in kind of retrofitting what we have versus trying to build these protections in as new technologies and new components of the grid are rolled out. And I don't know if there is any way you can quantify or address it in some other fashion. Yes.

Ms. SUGG. So you're right. The bulk of the standards and requirements are retrofitting to mitigate risks and identify and manage vulnerabilities and what not.

I applaud NERC's efforts to get ahead of the supply chain challenges that we have to develop standards. You know, the industry itself has moved forward.

The ISO/RTO council has put specific requirements in place for our control system vendors ahead of there being a standard that says you should have some secure coding practices for your control system vendors.

But it's not just software vendors. It's also hardware vendors. And then a comment made earlier about, I think it was Dr. Beck, about the importance of educating the consumer on those smaller devices.

I think we should put more emphasis on the manufacturers as well and really hold them accountable for developing things that are easy to maintain security with, not things that you just plug in and forget about, with the control systems and all of the systems within our organizations, not just those that NERC has put some mandated controls around but for all of those systems.

We have a responsibility and accountability to keep them current and to address vulnerabilities at all times. But that doesn't exist, to my knowledge, when you get outside of the industry.

And so I think we have to go back to the manufacturers and perhaps the equipment needs to be certified or——

Mr. SARBANES. Is it feasible to think in terms of, in a sense, cordoning off some of the consumer component of this internet of all things grid that's developing from more of the traditional infrastructure as a practical matter?

Do we just have to accept the notion that somebody's thermostat somewhere in their house can be a path all the way to shutting down some regional generator or something?

Mr. CAULEY. I think to a large extent we do that already because the most critical assets are in the bulk power system.

So you can picture a grid with the major control center and a lot of substations. We are trying to firewall it off, import multiple layers of protection.

So the image that comes to my mind is sort of a shuttle going through space and it's just getting bombarded all the time. So we are getting bombarded all the time and they are usually hitting the shield.

And as was mentioned earlier, sometimes the frailty is a human being enables something to get through. But so we are doing that.

A long-term question as a country that you're kind of raising, which is a lot of the electronics comes with huge capabilities. We used to buy a relay for the system and it would just be a couple of contacts and a coil of copper wire.

Now you get a box and it has 10,000 lines of code because it can do anything and everything that you want. Well, that philosophy really permeates everything in the consumer side, in the distribution systems and in the bulk power system.

We are getting electronics that can do everything. The difficulty there is then it can be reprogrammed to do anything anyone else wants.

All right. So I think we have to think about long-term partnership with suppliers, vendors, and manufacturers in terms of building better security into systems, making sure we are able to manage a purpose and have those be beneficial purposes and not adverse purposes.

Mr. SARBANES. Right. You have kind of a bundling problem. Get this thing and it can do all of this neat stuff that I don't necessarily need and could introduce a vulnerability that I won't notice because I never use that feature.

Mr. AARONSON. Just to sort of piggyback on some of that, I think we don't have the luxury of doing the ostrich thing and putting our heads in the ground.

Smarter energy infrastructure is here to stay and it serves a really important purpose and I think customers and consumers want it and are going to deploy and, again, utility scale and just industry in general sees the value.

We talked about distributed resources, having a impact on resiliency. They are both a good one and a bad one, and I think instead of trying to fully cordon off I think the most critical assets instead we need to look at segmentation and awareness of the vulnerabilities that are introduced and additional resilience to ensure that a problem at one node is not a catastrophic problem, more broadly.

And again, I think some of the standards that are already in place and some of the approaches to the promulgation of distributed resources are going in the right direction.

Mr. SARBANES. I yield back. Thanks.

Mr. OLSON. The gentleman yields back. The chair calls upon the gentleman from West Virginia, Mr. McKinley, for 5 minutes.

Mr. MCKINLEY. Thank you, Mr. Chairman.

This issue has come up literally every year since I've been in this committee for the last 6 years and I keep being told that everything is going to be fine, that we have got things under control.

Two years ago we had Tom Siebel with C3 Energy testify before us and Mr. Siebel said, it was kind of shocking to me, he said, I could—any hostile country—and he said as a matter of fact I could take 10 engineers from U.C. Berkeley and I could shut down the electric grid between Boston and New York within four days.

Now, that was after all the testimony about all the safeguards we had in place. So is Mr. Siebel wrong?

Mr. AARONSON. So I guess I'd push back on the premise a bit. He is not wrong in that, and I don't think any of us today are saying it's 100 percent under control.

I think, as I mentioned, it is an ongoing effort to continue to improve our defenses to respond to incidents internationally and domestically and to apply those here. You have two options.

You can be a good example or you can be a cautionary tale and, fortunately, there are a lot of cautionary tales out there about how a sophisticated, well-informed threat actor with a purpose can have an impact on grid operations.

I think what I would say is while an attack that has an impact is always within the realm of the possible, the resilience and redundancy that has grown up and the ability to respond that continues to evolve makes me a lot more comfortable in our ability to deal with these.

Mr. MCKINLEY. We took that theme, that concept back—we had a cybersecurity summit back in West Virginia and we had some 180 people attending, almost 200 people, in panels from all across the country, people coming in.

They all agree that we are still very vulnerable. This exercise that we go through, talking about and telling us we are OK. They are saying from the inside we are not.

So I am still going to remain uncomfortable—it goes back a little bit to what Johnny Wooden used to say when he was coaching the UCLA Bruins, that we often in America confuse effort with accomplishment. And I am afraid we are doing an awful lot of effort.

We are showing up daily, talking about it. But I am not comfortable yet and neither were the other people on the panel that we hosted.

So if I could now go to Ms. Sugg. One of the other testimony we had not too long ago here was from PJM and they said notwithstanding the problems that we have with cybersecurity but the bigger issue that we have with our electric grid is the electric magnetic pulse, EMP.

Do you agree with that, that it's as much of a threat as cyber, or worse?

Ms. SUGG. I think the probability of that occurring is much lower. However, the impact of it, if it were to happen, is much larger than a cyber-attack. So it is a concern.

We are working with the vertically integrated utilities who actually own the physical equipment to understand what sort of protections and redundancies and things that they need to have in place.

Our dependency on the telecommunication industry is certainly a concern there because if there were a significant EMP event it would take out the telecommunications.

And while we have a lot of redundancy in telecommunications, if it were all to go out then we'd have to relinquish the controls that we have back to the utilities themselves to help manage the grid.

But I know Dr. Beck is an expert on the EMP. I'll be interested in his additional comments.

Mr. MCKINLEY. If you could. We are running out of time on this.

Dr. BECK. Sure. Well, just quickly, they are both definitely an issue. We will just say on the one hand we have cyber-attacks, which are happening right now while we are having this conversation, right, versus EMP attacks getting the bullet for the EMP attack is difficult whereas getting the bullet for a cyber-attack you can go out and buy it right now on any criminal hacker web site.

So there is a much different proliferation concern. The footprints could be quite similar. You can distribute a cyber-attack quite broadly as you could with an HEMP attack and also the similarity in that similar types of systems can be attacked. Any computer network could be susceptible to any EMP. It could be susceptible to cyber.

Mr. MCKINLEY. In respect for the time I had some other questions. Let me just close with a—I would hope, given the confusion out there, that we could possibly just show us what accomplishments, if periodically we get briefed on different terrorism attacks.

If 56 were stopped last month or somehow to show that whatever you're doing on cybersecurity is working. Because when I have these panels they don't think it is.

So I need to have something back to be able to support that. Thank you. I yield back.

Mr. OLSON. Gentleman yields back.

The chair calls upon the gentleman from Ohio, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman, and I want to thank the panel for being here with us today.

Mr. Aaronson, some have expressed concern that the recent episode with the electric utility in Vermont will cause industry officials to avoid or think twice about sharing information with the government in fear that it could be leaked.

Trust, as we all know, is a two-way street, and while we need to ensure that industry officials are properly implementing and carrying out federal cybersecurity standards and regulations, the government must be a trustful cooperative partner.

What can be done, in your opinion, if anything, to improve this relationship and build trust, moving forward?

Mr. AARONSON. I appreciate the question. The first thing I'll say is it would be helpful if sensitive information shared in confidence was not shared then with the media.

Mr. JOHNSON. Hope you're better at it than we are here. Go ahead.

Mr. AARONSON. Well, I will say up to the moment that there was a front-page article in the Washington Post, I would suggest that the information sharing associated with the Vermont incident went perfectly.

There was actionable intelligence from government officials, shared with the Sector Coordinating Council. We brought together more than 30 CEOs onto a phone call within about 4 hours.

That information was then cascaded broadly throughout the sector at a very senior level and at the operative level both through the Sector Coordinating Council and the E–ISAC. Utilities across the sector took that information, compared it against their systems and what do you know, some potential indicators of compromise were found. That is exactly the way it's supposed to happen.

To answer your question about will this have a chilling effect on information sharing, I don't believe it will. I think because of the industry's commitment to and responsibility to help each other as we operate this one big machine together, there is a sense of responsibility to continue to share information even in the face of potential breach of or a potential disclosure to public sources.

But we are looking at what happened at the end of last year as a teachable moment and one that we hope isn't replicated. And I will give the Burlington Electric Department a ton of credit. They said in their statement that they would not let this episode chill their intent to continue to share information.

Mr. JOHNSON. OK. Good. Well, thank you for that. Anybody else want to comment on that? I've got a couple of other questions. OK.

Let's talk about information sharing a little bit and we will just go down the line for any that want to respond.

Why do you think situational awareness and information sharing is so necessary to enhance the electricity sector's ability to prepare for and respond to cyber and physical threats and vulnerabilities?

So why is situational awareness and information sharing so necessary? Mr. Cauley.

Mr. CAULEY. I think the main reason is that one company's only going to view their own experience and what they see. So if a company has one laptop compromised they think, well, that laptop got compromised, somebody must have pushed the wrong button.

But we are able to put together hundreds of specific instances, look at patterns over time and I think one of the capabilities we have through CRISP and through our analytics is to see patterns of connection points of internet locations, signatures of compromise, and things like that.

We can see a pattern over 3 months, 6 months, 18 months in some cases and you can see what they are doing. You can actually watch what's evolving in a very big picture.

So I think that's really the multiplier effect of being able to get everybody's data and to be able to share. We share through the DOE lab. We work the CRISP program.

On the back end of that is the Pacific Northwest lab. They have people working classified space, helping us analyze the data. So for us to be able to get that, what does it mean, what are people trying to do to us, what should we look for, we turn around and give that back to industry.

Mr. JOHNSON. OK.

Mr. AARONSON. In the interest of time, I will say Gerry is spot on and I would just add one more thing Ms. Sugg said earlier which is, I love this quote, I wrote it down: "Someone's detection is someone else's protection."

And I think everything that happens is a lesson for the rest of the industry. Applying it helps make us all more secure.

Mr. JOHNSON. See something, say something.

Mr. AARONSON. There it is.

Mr. JOHNSON. There you go.

Dr. BECK. I think situational awareness, even in the broadest terms, is important. So whether knowing about a certain attack at a certain utility, that whether or not it needs to be defended against by a different utility it's just important to have visibility to those reports to understand, this situation is happening or the frequency of attacks or that people are reporting it I think that just raises the consciousness of keeping your eye on this particular ball.

Mr. JOHNSON. OK. Ms. Sugg.

Ms. SUGG. Very quickly, the NERC alert system certainly has picked up in frequency of alerting. As Mr. Cauley mentioned earlier, given the understanding that we need to be thinking about events at any level no matter how small, one of the things that makes it particularly useful to us, I believe, is the accountability to respond to it.

So it's not just a matter of, oh, I received some information and maybe I'll study that someday. But NERC puts requirements around—you must read this, you must look at these things and you must report back, and I think that that helps to ensure that if there are vulnerabilities somewhere that some utility has found that they are responsible for addressing those and reporting that back to NERC.

Mr. JOHNSON. OK. Great. Mr. Chairman, I yield back. Thanks for indulging.

Mr. OLSON. Gentleman yields back. The chair calls upon the gentleman from Michigan, Mr. Walberg, for 5 minutes.

Mr. WALBERG. Thank you, Mr. Chairman, and thanks to the panel for being here.

Coming from Michigan and my district, bordering Canada, I was just interested to know that since this grid is a North American grid, could you please describe, Mr. Aaronson, how utility industry coordinates with our northern neighbors on cyber and grid security.

Mr. AARONSON. Sure, and I'll rely on Gerry a little bit, too, given NERC's responsibility as the North American Electrical Reliability Corporation.

For the Sector Coordinating Council, the Canadian Electricity Association has been a integral part of that relationship as has the Canadian government. We have had not just the Department of Energy and Department of Homeland Security here in the United States but Natural Resources Canada and Public Safety Canada, their counterparts respectively north of the border.

Given that this is a North American grid, we are all operating the same machine together, number one. Number two, you've seen in instances of particularly natural disasters where it's not just crews and bucket trucks from the United States descending on affected areas but from north of the border as well.

And then also with our nascent, but growing cyber mutual assistance program, there have been Canadian utilities as part of that relationship also.

Mr. WALBERG. Mr. Cauley.

Mr. CAULEY. So to us they are equally engaged in all of our programs. We actually have representation on the coordinating council at the CEO level.

They participated in the ISAC. They follow our standards and so they are equal partners. We share information with them. They've had some things happen in Canada that we have not seen, like an airplane flying over lines and dropping wire on line.

So somebody was disgruntled and decided to launch their own attack out of an airplane. But we share that among ourselves and we are able to basically learn from each other and they are equal partners and I think all the ISOs in Canada are run highly competent systems with the similar controls we have on the U.S. systems.

Mr. WALBERG. Continuing on, Mr. Cauley, with some concerns about the relationships with Canada and ourselves from my state specifically, there is a growing number of interdependencies between power generation and natural gas, pipelines included.

The two industries are similar but are different in some ways. How are you addressing power generation resilience to avoid single points of failure and what opportunities do you see, moving forward?

Mr. CAULEY. It's a very timely topic for us. We have actually been doing some recent analysis and we are in the processing of publishing a report to look at key parts of the gas infrastructure system that we depend on.

We have now three of our eight regions that have more than 50 percent of the power supplied by natural gas. And so pipelines and storage facilities do create vulnerabilities and I think not just from a physical perspective in terms of competition with retail gas cus-

tomers in extreme weather but also from a cyber perspective where physical attack disruptions could cascade over into electric power.

So it's high on our list of priorities and the one thing we do encourage is diversity in fuel and we encourage infrastructure and I think this is the partnership between us and Canada and the growing partnership with the infrastructure in Mexico which we are involved in will help us ensure our energy security through exchange of gas and electricity and renewables and all kinds of resources.

Mr. WALBERG. And, hopefully, along with that concept, moving back to a more robust standard of all of the above in generation and fuels.

I know there has been a push that's pushed, at least in my district, the energy district of the state, away from having that robust opportunity for an all above standard.

Mr. Cauley, let me just in the remaining few seconds here, how is NERC and the industry working to develop policies to encourage use of system components that will be less vulnerable to attack?

And follow that up, what the Department of Energy is doing in this front as well and how you're working with them?

Mr. CAULEY. Well, our standards, and I think the experience that we are learning with feeding back industry encourage better protection.

One of the things that we are seeing directly is greater diversity of equipment and basically reducing the criticality of an individual station or piece of equipment and creating redundancies in the system to make us less vulnerable.

So I think there is a lot of examples like that where people are reacting to being more secure and building it into the architecture and design of their systems.

Mr. WALBERG. I yield back.

Mr. OLSON. The gentleman yields back.

We saved the best for last. The chair calls upon the gentleman from Ohio, Mr. Latta, for 5 minutes.

Mr. LATTA. Well, thank you very much, Mr. Chairman, and to the panel thanks very much for being here today. It's very, very informative.

I know that the other juries that we have had in the past year and two, I should say, that you know, this is a very, very important topic.

It's a very, very serious topic, and if I could start with you, Mr. Aaronson, if I could ask this. You mentioned in your testimony that you're working with DOE to determine the scope and process for emergency orders.

Would you expand on that conversation and provide insight as to whether there would be further action from Congress at this time?

Mr. AARONSON. I don't know about further action from Congress yet. I mentioned earlier that the notice of proposed rulemaking was put out a few months ago.

We have a due date actually of this coming Monday, February 6th, to get comments in. Those comments are helping to inform the process of what an emergency order from the Secretary of Energy might look like.

I think the most important thing, and it is built into the NOPR, is this idea of consultation. The law said consultation with the sector where practicable.

Practicable to us is a little concerning, given that any emergency order that doesn't take into account how grid operators actually operate the system could have unintended consequences.

So that is a point that we are making in this response to the rulemaking to help inform the process. But I do think that given all of the great relationship we have with the secretary of energy and, frankly, just the Department of Energy in general as our sector-specific agency we are confident that they understand us, we understand them and think we can work productively with them to implement that emergency authority.

Mr. LATTA. OK. Thank you. Let me follow up, and this has been touched on a little bit before. You said something kind of interesting that I wrote down.

You mentioned earlier about the vulnerabilities that the—that are potentially a concern through the internet of things, and if you could expand a little bit on that work and also with the electricity infrastructure sharing and analysis center and beginning to fix those risks.

But then you said this. I thought, this is kind of interesting. You said you were on a journey without a destination. That's not real comforting as we are going down that road.

Mr. AARONSON. Maybe I should pick a better cliche.

Mr. LATTA. I write those things down.

Mr. AARONSON. But the point I am getting across is there is no such thing as 100 percent security. So we are constantly evolving and I think that is a good thing.

If we became stagnant and just relied on this culture of compliance and, yes, we are secure, we would not be able to be responsive to new and emerging threats.

So, it's the old joke—I don't have to be faster than the bear, I just have to be faster than the other guy. There is another cliche to add to that—the hit list.

But what we were doing is constantly trying to stay ahead of the adversary and they have intent and capabilities but we do too.

And I think I am particularly proud of the industry's culture of constantly reinventing and looking at its security posture, seeing where there are gaps, using exercises like GridEx, using observations from things that happen overseas and here at home and learning from those and then applying them to make us better.

And to Mr. McKinley who I am sorry isn't here, I agree I love the wooden quote of effort does not equal accomplishment.

But I would say there have been a number of accomplishments from putting in place spare equipment programs to creating a cyber mutual assistance program to doing a better job of sharing information to developing the cyber risk information sharing program and applying it from a DOE lab into a commercial application.

So a lot of stuff that is happening in a very short amount of time because of the CEO leadership of the Sector Coordinating Council.

Mr. LATTA. Thank you. Ms. Sugg, if I could go back to what you also said. You said that innovation is important. Are we meeting

that innovation to make sure we keep up the standards to make sure that we meet these potential threats?

Ms. SUGG. Well, innovation is certainly changing faster than the standards are changing, hence my comments about ensuring that the standards are not overly prescriptive but are more focused on the risk.

Innovation is important whether it be trying to understand the threat avenues from our attackers or understanding the newer and more interesting technologies that are coming to bear that may provide some additional securities for us beyond what we have today.

We don't ever want to be really comfortable with our architecture that we have in place. We need to continue to look at opportunities to strengthen it, depending on what technologies are available and matching that up with where the threats seem to be coming in and how we can try to get ahead of that.

Mr. LATTA. Thank you.

Mr. Chairman, my time has expired and I yield back.

Mr. OLSON. Gentleman yields back and the chair would like to have one invitation for the witnesses.

If you want to see a robust grid security in action at a small level, come to Houston, Texas this weekend. There is this big football game called Super Bowl 51. It's not a power grid, but as you can imagine, if the power goes down right as the Falcons are about to score that touchdown to beat the Patriots, there will be a riot of biblical proportions. Invitation does not come with tickets, and that'll cost you a pretty penny.

But seeing no further members wishing to ask questions, I want to thank all of our witnesses for your participation in today's hearing.

And pursuant to committee rules, I remind members that they have 10 business days to submit additional questions for the record and ask the witnesses to submit their responses in 10 business days upon receipt of the questions.

Mr. Rush, before you leave I ask for uanimous consent that a statement for the record from the Large Public Power Council and a statement from the American Public Power Association and NRECA be put in the record.

Without objection, the subcommittee is adjourned.

[Whereupon, at 12:49 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

CELEBRATING
30 YEARS
LPPC
LARGE PUBLIC POWER COUNCIL

Statement of the
LARGE PUBLIC POWER COUNCIL

Submitted to the
HOUSE ENERGY AND COMMERCE SUBCOMMITTEE ON ENERGY

Hearing on
"The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

February 1, 2017

The Large Public Power Council ("LPPC") submits this statement to the House Energy & Commerce Committee's Subcommittee on Energy ("the Subcommittee"), in connection with the hearing on "The Electricity Sector's Efforts to Respond to Cybersecurity Threats." to be held February 1, 2017. LPPC is an association of the 25 largest state-owned and municipal utilities in the nation. LPPC members are located throughout the nation, both within and outside RTO boundaries. LPPC represents the larger, asset-owning members of the public power sector. Together, they own roughly 90% of the electric transmission investment owned by public power entities in the United States.

LPPC supports the Subcommittee's interest in being fully informed regarding the cyber threats facing the electric industry, and the industry's response. LPPC members are acutely aware of the risks facing the industry and are actively involved in efforts within their companies

and at the governmental level to manage risk and respond to known and emerging vulnerabilities. The attack on the Ukrainian electric grid, mentioned in the Majority Staff memorandum submitted to the Subcommittee in connection with this hearing, is certainly an indication that the industry must be vigilant.

Yet, LPPC urges the Committee to take stock of the measures that have been taken by the industry, the North American Electric Reliability Corporation ("NERC") and the government to respond to these risks. The focus of this statement is on those measures, including: (1) the mandatory standards regime administered by NERC; (2) the reliance by the industry on a range alternative frameworks and resources to evaluate vulnerability and anticipated response; (3) reliance on the Electric Sector Information Analysis Center ("ES-ISAC"); (4) existing government-industry partnerships; and (5) the range of mutual assistance programs relied on by the industry to enhance security.

1. NERC's Reliability Enforcement Regime

Cybersecurity measures undertaken by the electric industry areas are governed by a suite of mandatory Critical Infrastructure Protection ("CIP") standards promulgated by NERC and approved by the Federal Energy Regulatory Commission ("FERC"). The electric sector is the only sector of the economy that operates under mandatory, enforceable standards. NERC's CIP standards adopt a risk-based approach that begins with an inventory of critical assets, and attaches a comprehensive suite of protective measures encompassing security management controls, personnel and training, electronic security perimeters, physical security, system security management, incident reporting, response planning and recovery.

Though the electric industry is involved in the development of the NERC standards through an ANSI-approved process, it does not control the nature of the standards ultimately

submitted by NERC for approval by FERC, or FERC's oversight. Enforcement of the standards by both NERC and FERC is entirely independent of the industry. Under the Federal Power Act (FPA), FERC's certification of NERC as the Nation's Electric Reliability Organization (ERO) was contingent on its development of rules assuring its independence from "users and owners and operators of the bulk-power system." Further, FERC has the authority to order NERC to submit to the Commission proposed reliability standards or modifications to reliability standards that address vulnerabilities identified by the Commission.

2. Reliance on Other Government-Sponsored Reliability Frameworks

LPPC participated directly, along with others in the electric industry, in the process leading to the development of the Cybersecurity Framework promulgated in 2014 by the National Institute of Standards and Technology, following a Presidential Directive. As well, LPPC members closely followed the development of the Department of Energy's Cybersecurity Maturity Model. Both of these frameworks provide models for the evaluation of cybersecurity vulnerabilities, and processes for risk management aimed at continuous evolution and improvement. LPPC members routinely use these tools to evaluate their cyber programs from various perspectives independent of the NERC CIP standards, and to strive for continuous improvement.

3. Information Sharing and Alerts Through the E-ISAC

The electric industry's primary resource for sharing information of cyber threats—with the government's encouragement—is the E-ISAC. Administered by NERC, and operated in coordination with the Electric Sector Coordinating Council (ESCC) and the Department of Energy, the E-ISAC was chartered to facilitate sharing of information regarding physical and cyber threats, vulnerabilities, incidents and potential protective measures. It serves as the primary security communications channel for the electricity sector, coordinating communications

by and between members companies, sharing campaign analysis and incident data from private and public entities and it coordinates event and threat analysis with DOE, FERC and DHS. The E-ISAC was launched following the issuance of Presidential Decision Directive 63 (PPD-63), along with nearly a dozen other ISACs operating critical infrastructure in other sectors of the economy. The E-ISAC is among the most robust and effective of these organizations and the electric industry's vehicle of choice for information sharing.

4. Partnership with the Government

At the most senior levels, the electric industry is in close contact with the government through the Electric Sector Coordinating Council ("ESCC"). The ESCC serves as the principal link between the Administration and high-level electric industry executives. It is populated by Cabinet-level members from DOE and DHS, senior electric industry executives and trade association leaders. As are other sectors of the electric utility industry, LPPC is represented on the ESCC and values the direct contact it offers, enabling the Administration and industry to share information regarding ongoing and anticipated risks, and recommended responses. The forum provides an invaluable communication tool.

These contacts extend to other levels of government. The electric industry is in close contact with officials at the Department of Energy working on grid security (the Office of Energy Policy and Systems Analysis and the Office of Electricity and Energy Reliability) and the Federal Bureau of Investigation. Further, industry officials routinely coordinate with states, municipalities and local governments in order to maintain the most comprehensive view of threats, risks and vulnerabilities.

5. Voluntary Mutual Assistance

Along with other members of the electric industry, LPPC members routinely rely on voluntary industry associations for the purpose of strengthening their approach to cybersecurity.

Best practices are shared through the North American Transmission Forum and the American Public Power Association's "Improving the Cyber Resiliency and Security Posture of Public Power" (sponsored by the Department of Energy). LPPC has created its own Cyber Security Task Force, charged with the responsibility of sharing best practices, serving to disseminate news of emerging risks, and helping to advocate public policy solutions,

Also of note, following NERC's Grid-Ex incident response exercise, the ESCC established the Cyber Mutual Assistance Task Force, an organization that has convened industry experts to develop a mutual assistance program for cyber threats, aimed at assisting electric utilities to rebuild and recover necessary computer systems in the event of a regional or national cyber incident. The Task Force also aims to provide shared educational assistance and training to facilitate the provision of mutual assistance in the event of an emergency.

The electric industry's response to cyber risks is robust, fast-evolving, and intimately tied to efforts by the government to enhance the nation's security posture. We welcome the opportunity to work with members of the Subcommittee to provide further information, and to receive their input in this joint endeavor.

John DiStasio
President
Large Public Power Council

Joint Statement for the Record by the

AMERICAN PUBLIC POWER ASSOCIATION (APPA) and the

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION (NRECA)

Submitted to the

HOUSE ENERGY AND COMMERCE SUBCOMMITTEE ON ENERGY

For the February 1, 2017, Hearing on

"The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

The American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) appreciates the opportunity to submit a statement for the record for the House Energy & Commerce Committee's Subcommittee on Energy hearing on "The Electricity Sector's Efforts to Respond to Cybersecurity Threats." APPA and NRECA supports and agrees with the testimony of Mr. Scott Aaronson of 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 cyberattacks directed at the grid.

The Energy & Commerce Committee developed important grid security provisions in the comprehensive energy bill that were ultimately passed into law as part of H.R. 22, "Fixing America's Surface Transportation Act" ("FAST Act"). These provisions included establishing DOE as the sector-specific agency (SSA) for the electric utility industry, giving DOE authority to direct industry to take action in the event of a grid security emergency, protecting critical electric infrastructure information (CEII) from public disclosure and devising a plan for a spare transformer program. We appreciate and applaud the hard work that went into moving these issues forward.

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.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

February 23, 2017

Mr. Gerry W. Cauley
President and CEO
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005

Dear Mr. Cauley:

Thank you for appearing before the Subcommittee on Energy on Wednesday, February 1, 2017, to testify at the hearing entitled "The Electricity Sector's Efforts to Respond to Cybersecurity Threats."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on March 9, 2017. Your responses should be mailed to Will Batson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Will.Batson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Fred Upton
Chairman
Subcommittee on Energy

cc: The Honorable Bobby Rush, Ranking Member, Subcommittee on Energy

Attachment

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 10, 2017

The Honorable Fred Upton
Chairman
Subcommittee on Energy
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Chairman Upton:

On behalf of the North American Electric Reliability Corporation, thank you for inviting me to testify before the Subcommittee on Energy on Wednesday, February 1, 2017, at the hearing entitled, "The Electricity Sector's Efforts to Respond to Cybersecurity Threats." Attached are my responses to questions for the record.

Again, we greatly appreciate the opportunity to support the important work of the subcommittee.

Sincerely,

Gerry W. Cauley
President and Chief Executive Officer

cc: The Honorable Bobby Rush, Ranking Member, Subcommittee on Energy

Attachment

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

Responses from Gerry W. Cauley
President and CEO
North American Electric Reliability Corporation

Subcommittee on Energy Hearing
"The Electricity Sector's Efforts to Respond to Cybersecurity Threats"
February 1, 2017

Additional Questions for the Record

The Honorable Fred Upton

1. One of the challenges the electric sector faces appears to stem from harnessing digital technology onto industrial control systems and other components that were not designed to account for the risks modern malware and digital communications may create.

A. Explain how NERC and industry are working to develop policies to encourage development of system components that will be less vulnerable to attack?

NERC and industry have several ways in which we are developing and supporting policies related to strengthening system components. NERC's robust Critical Infrastructure Protection (CIP) standards are designed to protect critical electric infrastructure, thereby resulting in procurement of advanced technologies necessary to comply with CIP requirements. In addition, FERC ordered NERC to develop a new CIP standard to address supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.

NERC also has a standing technical committee, the Critical Infrastructure Protection Committee (CIPC), that helps NERC advance the physical and cyber security of the critical electricity infrastructure of North America. The committee consists of both NERC-appointed regional representatives and technical subject matter experts. CIPC coordinates NERC's security initiatives and serves as an expert advisory panel to the NERC Board of Trustees, standing committees in the areas of physical security and cybersecurity, and the Electricity Information Sharing and Analysis Center (E-ISAC).

NERC's E-ISAC works closely with the Electricity Subsector Coordinating Council (ESCC), supporting policy development efforts through the ESCC's various working groups. The ESCC's Research and Development Working Group collaborates closely with the Department of Energy (DOE) on initiatives to address strengthening system components.

NERC recently shared information with industry concerning the Internet of Things (IoT) vulnerability. On October 11, 2016, NERC issued a non-public Level 2 Alert, "Internet of Things (IoT) Used for High Bandwidth Distributed Denial of Service (DDoS) Attacks." Also, the E-ISAC published an Internet of Things DDos White Paper on October 24, 2016, providing recommendations for

defensive capabilities in the Electricity Subsector, with suggestions for improving the overall posture of network security and cybersecurity.[1] NERC also issued a non-public Level 2 Alert with recommendations on February 9, 2016, regarding the events that occurred in Ukraine, followed by the posting of the joint team analysis on March 21, 2016, to provide a lessons learned resource from event. These efforts help to inform industry about the vulnerabilities in system components that were vectors in those attacks.

i. What is the Department of Energy doing on this front and how are you working with DOE?

The U.S. Department of Energy (DOE), the National Institute of Standards and Technology, and trade organizations from the electric power and manufacturing industries have developed best practices and guidelines, which cover various procurement and supply chain cyber security risk management practices.

DOE's Office of Electricity Delivery and Energy Reliability has developed the Cybersecurity Capability Maturity Model (C2M2). C2M2 is a voluntary evaluation process utilizing industry-accepted cybersecurity practices that can be used to measure the maturity of an organization's cybersecurity capabilities. The C2M2 is designed to measure both the sophistication and sustainment of a cyber security program. The model was identified, organized, and documented by energy sector subject matter experts from both public and private organizations.[2] NERC provided DOE with technical expertise and industry outreach support during development of the C2M2 model.

In addition, DOE and NERC regularly work together to provide threat and vulnerability briefs to stakeholders. Several DOE presentations on supply chain issues, as well as research and development (R&D) programs, have been briefed to industry stakeholders at NERC conferences, including National Laboratory projects and the Cybersecurity for Energy Delivery Systems (CEDS) R&D program. NERC and the E-ISAC collaborate often with DOE and their national labs systems on a regular basis. For example, DOE provided input helping support the E-ISAC in development of the GridEx IV scenario. The E-ISAC and DOE also coordinate during regular synch meetings to discuss current threats and vulnerabilities.

B. What is NERC doing, what is the industry doing, to encourage development and procurement of so-called secure by design control systems-those designed to be more invulnerable to cyberattacks?

NERC encourages industry participation in security-related pilot programs and broader efforts through DOE and other sources to increase protection from cyber attacks. Some programs include the California Energy Systems for the 21st Century (CES-21) program, the Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program, and others. NERC facilitates sharing

---

[1] *The white paper is posted to the E-ISAC website at* https://www.eisac.com/.

[2] *See DOE fact sheet at* https://energy.gov/sites/prod/files/2014/02/f7/C2M2-FAQs.pdf.

technology briefs about these programs with stakeholders, and is working with the RADICS team to deploy tools to industry in conjunction with GridEx IV and V.

Industry participants have also worked with the Department of Energy to draft the DOE guidelines on *Cybersecurity Procurement Language for Energy Delivery Systems* (https://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014). Further, the Edison Electric Institute developed a set of key principles and recommendations for entities to consider for managing supply chain cybersecurity risks (http://www.eei.org/issuesandpolicy/testimony-filings-briefs/Documents/150917FinalEEIPrinciplesandResourcesforManagingSupplyChainCybersecurityRisk.pdf).

i. What is the state of research on this front?

NERC would defer to the Department of Energy as well as the Electric Power Research Institute (EPRI) on this question.

ii. What are the barriers to deployment?

From NERC's standpoint, one challenge for deployment of new technology is that it must be proven to be reliable over time in a variety of conditions. In addition, the full consequences of the use of new technology must be understood. Because the electricity system is an interconnected network, any changes in one component may have consequences for the use or operation of other components.

The Honorable Morgan Griffith

1. Today, the electric industry works with the DOE, with DHS, with the FBI, and other agencies to share information on threats and intelligence. But there does not appear to be a coordinated way for industry to share or receive information across these agencies, leading to more individualized notices from agencies than may be desirable.

A. How can the federal government ensure better coordination within its own agencies and with the electric industry regarding information on threats and intelligence sharing?

The E-ISAC is a leading, trusted source for the analysis and sharing of electricity industry security information. The E-ISAC reduces cyber and physical security risk to industry across North America by providing unique insights, leadership, and coordination. One of the E-ISAC's central roles is to connect industry and government. To accomplish this, the E-ISAC works closely and regularly with the National Cybersecurity and Communications Integration Center—the central means for the federal government to aggregate and share information on cyber threats. In addition, NERC works closely with the ESCC to further the public private partnership dialogue addressing security and resilience matters. Maintaining this partnership is key to ensuring private and public sector communications regarding threats and intelligence sharing.

To achieve better coordination, the federal government can enhance the clearance process to ensure appropriate industry individuals are cleared at the appropriate levels to receive classified information and provide subject matter expertise. In addition, the government can work to downgrade classified information when feasible for industry that is timely and actionable. Finally, the government can assist industry by ensuring access to local classified briefing spaces so that industry subject matter experts can receive information and provide input and advice from an asset owner and operator perspective.

2. Some electricity utilities are participating in the Cyber Risk Information Sharing Program, which allows the utilities to send network data for analysis against government sources.

A. How can we expand programs like this to provide a frictionless partnership between the public and private sectors that allows private industry to be more agile in its response and allows the government a level of assurance that the power grid is secure?

CRISP is an important partnership between DOE, NERC and the industry, providing critical security information to entities serving 75% of electricity customers in the United States. NERC and the E-ISAC are working with DOE on other initiatives that may enhance the CRISP programs, including extending CRISP into the operational technology environment. DOE has also initiated a grant program with electricity industry trade associations focused on improving the cyber and physical security culture for members of the National Rural Electric Cooperative Association and the

American Public Power Association. The grant will develop security tools, provide educational resources, update security guidelines, and offer training.

In addition, the Department of Defense is partnering with NERC, the E-ISAC, and industry asset owners and operators to deploy and evaluate tools and technologies for grid security through the RADICS program.

The Honorable Frank Pallone

One emerging challenge in grid security relates to the thousands of businesses, vendors and suppliers that make up the electric sector supply chain. There are several high profile examples from the retail sector where breaches to such third-party entities ultimately have caused direct harm to the first-party organization.

Mr. Cauley, in your testimony, you mention that modification of the Critical Infrastructure Protection (CIP) Standards are under development to address such challenges in supply chain management.

1. Can you provide an update on the development timeline for any new requirements to the CIP Standards to address supply chain cybersecurity issues? In particular, when will such modification be finalized?

FERC Order No. 829, directs NERC to develop by September 27, 2017 a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. The new or modified Reliability Standard is intended to mitigate the risk of a cybersecurity incident affecting the reliable operation of the bulk power system. The order stated that the new or modified Reliability Standard should address the following security objectives: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. In FERC Docket No. RM15-14-002, NERC filed its complete project plan outlining the timeline for completing this standard.[3]

2. In light of these pending new requirements, what options or best practices are available now for utilities to ensure the cybersecurity of their supply chain partners?

Best practices and guidelines have been developed by the U.S. Department of Energy, the National Institute of Standards and Technology, and trade organizations from the electric power and manufacturing industries. These cover various procurement and supply chain cyber security risk management practices.

Some examples are:

Cybersecurity Procurement Language for Energy Delivery Systems
http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

Cybersecurity Procurement Language for Control Systems Version 1.8
http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SCADA_Procurement_Language.pdf

National Electrical Manufacturers Association (NEMA) Supply Chain Best Practices Guideline

---

[3] *See* http://www.nerc.com/pa/Stand/Pages/Project201603CyberSecuritySupplyChainManagement.aspx.

Document CPSP 1-2015
http://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx#download

Supply Chain Risk Management Practices for Federal Information Systems and Organizations
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

"Principles and Resources for Managing Supply Chain Cybersecurity Risk"
http://www.eei.org/issuesandpolicy/testimony-filings-briefs/Documents/150917FinalEEIPrinciplesandResourcesforManagingSupplyChainCybersecurityRisk.pdf

In addition, NERC continues to monitor and communicate the security risks posed to the Bulk Power System by the increased use of Internet of Things (IoT). On October 11th, 2016, NERC issued a non-public Level 2 Alert, "Internet of Things (IoT) Used for High Bandwidth Distributed Denial of Service (DDoS) Attacks." Also, the Electricity Information Sharing and Analysis Center (E-ISAC) published an Internet of Things DDos White Paper in October 24, 2016 providing recommendations for defensive capabilities in the Electricity Subsector, with suggestions for improving the overall posture of network security and cybersecurity.[4]

3. Do current cybersecurity standards address vulnerabilities to utilities posed by IoT devices?

The CIP standards afford protections and safeguards to the "Industrial" Internet of Things where over the past decade we have a observed a substantial increase in the number of intelligent devices deployed throughout the bulk power system that if compromised could have some real impacts to reliability. NERC's CIP standards have evolved to better address new and dynamic threats. Reliability Standards are a necessary foundation to address the vulnerabilities to utilities posed by IoT devices, but they are not sufficient alone to protect against these evolving threats. Monitoring and communication with timely information exchange is essential.

4. Will the update to the CIP standards to address supply chain cybersecurity also be sufficient for addressing risks posed by IoT devices? And if not, how must utilities adapt their cybersecurity measures to best protect themselves from the risks posted by IoT technologies?

FERC directed NERC to develop a standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. This standard is currently under development. Once approved by FERC, this standard would focus on the security of the products acquired by entities subject to the standard. Currently enforceable CIP standards requirements, which include methods to identify industry intelligent systems used to operate the grid, network security, malware protection,

---

[4] *The white paper is posted to the E-ISAC website at* https://www.eisac.com/.

incident response as well as other security controls, are in place to further protect assets being used to operate the grid.

In response to risks posed by IoT devices, and as noted above, NERC issued a non-public Level 2 Alert regarding the IoT vulnerability. The E-ISAC also published an Internet of Things DDoS White Paper to provide recommendations for defensive capabilities in the electricity sector and suggestions to improve the overall posture of network security and cyber security.

5. In 2016, roughly how many entities were in violation of the CIP standards, and roughly how many of these violations were specifically related to non-compliance associated with mandatory protections for cybersecurity?

In 2016, 128 registered entities reported noncompliance with CIP standards. This figure accounts for 10% of NERC registered entities subject to CIP standards. A majority of these reports are still under review.

The Honorable John Sarbanes

1. What technical or funding support are you receiving from federal agencies on grid cyber security in terms of research and development and standard setting guidance? How could this support be enhanced or improved?

NERC receives no funding from federal agencies. As noted in my testimony, NERC derives considerable technical expertise from federal agencies through partnerships and collaboration with DOE, DHS, and NIST. In addition, FERC provides technical expertise for a wide range of NERC activities through formal and informal means, including the reliability standard review process and many other programs. Continued support for these partnerships remains important.

The Honorable Jerry McNerney

1. The second installment of the QER noted that the traditional definition of reliability may be insufficient to ensure system integrity and available electric power in the face of physical attacks and cyber threats, among other things. And that the security of the system, particularly cybersecurity, is a growing concern. Would you agree with this assessment?

In the Energy Policy Act of 2005, Congress expressly included "cybersecurity protection" when it defined the scope of "reliability standards" in Federal Power Act (FPA) Section 215(a)(3). NERC agrees that physical and cybersecurity threats are a growing concern. NERC and our government and industry stakeholders have been and remain focused on them.

2. Is there a uniform definition used in the energy and electricity sector - or at the federal level - of what cyber "secure" or "resilient" means?

NERC defines security and resiliency through the use of our standards and information sharing efforts. As we have discussed, this is part of a collective approach to risk, with standards providing a strong foundation for a reliable and secure BPS.

3. How costly is it to fund research RD&D for cyber from a utilities perspective? When updating your networks and physical infrastructure, are you able to put in new, more cyber secure equipment in select areas or does it need to be done across the board? Do you feel that cyber security and resilient investments are adequately reflected in rate-making cases?

NERC defers to individual utilities to provide perspective on research funding and recovery of cyber and resilient investments in rate cases.

4. Are customers appropriately knowledgeable on cybersecurity? How do we address that shortcoming?

NERC's registry contains nearly 1,500 users, owners and operators of the Bulk Power System. Through the E-ISAC, NERC reaches even more electric system entities and provides them with information. This is an ongoing challenge, but working together with our federal government partners, with state regulators and with utilities, Regional Transmission Organizations, customers and experts, we are trying to increase the level of awareness of cybersecurity threats and what can be done to address them.

5. Given the dynamic changes happening at the distribution level, are there adequate measures in place across the country to ensure the same type of oversight and protection that occurs on the bulk power system? Are there ways for the distribution system to become a threat to the bulk power system reliability?

NERC's jurisdiction includes users, owners, and operators of the bulk power system (BPS). "Facilities used in the local distribution of electric energy" are excluded from the definition of the "bulk-power system" under FPA Section 215, and are regulated by the states. However, NERC's jurisdiction does extend to certain distribution providers connected to the BPS that impact over 300MW of

automatic load shedding. In other words, certain distribution providers that could impact reliable operation of the BPS are subject to CIP standards.

E-ISAC's information sharing portal has reach to distribution providers. While NERC's jurisdiction is focused on the BPS, all distribution providers are eligible to become members of the E-ISAC portal, even distribution providers that are not connected to the BPS. Therefore, distribution providers that are members of the E-ISAC portal benefit from cyber and physical security information from the E-ISAC.

NERC recently issued the Distributed Energy Resources Connection and Modeling and Reliability Considerations assessment. The report discusses potential reliability risks and mitigation approaches for increased levels of distributed energy resources on the BPS. DER will increasingly have state-of-the-art capabilities for active power control and reliability services. However, there are differences in how DER are deployed within the grid and the characteristics of the services and responses that they provide, so these differences must be understood and modeled appropriately. As a result, this report explains how practices for modeling and operating the BPS may be enhanced to reflect future system characteristics. It is paramount that NERC and the industry understand DER functionality and develop a set of guidelines to assist in modeling and assessments such that owners/operators of the BPS can evaluate and model DER in the electric system. The report is meant to help entities, regulators, and policy makers better understand the differences between DER and conventional generation and how DER affect the BPS.

6. Most outages occur on the distribution side and not the bulk power system. It's my understanding that NERC uses a number of indicators, like the System Average Interruption Duration Index, which is calculated on a monthly or yearly basis.

SAIDI (System Average Interruption Duration Index) and SAIFI (System Average Interruption Frequency Index) are metrics that are widely used by industry to assess reliability on their distribution systems. As NERC's focus is on the BPS, NERC utilizes the SRI, or Severity Risk Index. The SRI is a measure of stress to the BPS in any day resulting from generation loss, transmission loss, or load loss components. The SRI is a key metric in NERC's annual State of reliability report which assesses the reliability performance of the BPS.

7. You mentioned that the GridEx III participants were encouraged to share lessons learned. Out of the thousands who were involved, how many provided the feedback you asked for?

Thousands of individuals participated in GridEx III. In collecting responses from industry, the E-ISAC focused on obtaining feedback from organizations and lessons learned that had not been identified in previous exercises. NERC issues a public report after each GridEx.[5] For GridEx III, NERC received 25 lessons learned reports, representing about 24 percent of active participating utility organizations. These lessons learned represent opportunities for industry to identify possible initiatives to enhance response to cyber and physical attack or improve future exercises of this nature.

---

[5] *See GridEx III report at* http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx.

Voluntary submissions from organizations have continued to increase with each successive GridEx exercise. We anticipate this trend will continue.

8. Your testimony stated that there has been no loss of load due to a cyber-attack. Would you like to expand on that?

As you point out, there has not been any loss of load in North America that can be attributed to a cyber attack. This recognizes the commitment of industry and the effectiveness of complementary strategies discussed in my testimony. However, we cannot be complacent. We must remain vigilant in assuring the reliability and security of the bulk power system.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

February 23, 2017

Mr. Scott L. Aaronson
Executive Director
Edison Electric Institute
701 Pennsylvania Avenue, N.W.
Washington, DC 20004

Dear Mr. Aaronson:

Thank you for appearing before the Subcommittee on Energy on Wednesday, February 1, 2017, to testify at the hearing entitled "The Electricity Sector's Efforts to Respond to Cybersecurity Threats."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on March 9, 2017. Your responses should be mailed to Will Batson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Will.Batson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Fred Upton
Chairman
Subcommittee on Energy

cc: The Honorable Bobby Rush, Ranking Member, Subcommittee on Energy

Attachment

Responses from Scott L. Aaronson
Edison Electric Institute

Subcommittee on Energy Hearing
"The Electricity Sector's Efforts to Respond to Cybersecurity Threats"
February 1, 2017

Additional Questions for the Record

The Honorable Fred Upton

1. **One of the challenges the electric sector faces appears to stem from harnessing digital technology onto industrial control systems and other components that were not designed to account for the risks modern malware and digital communications may create.**

   Explain how NERC and industry are working to develop policies to encourage development of system components that will be less vulnerable to attack?

   The industry has been focused on managing and reducing risk associated with the use of digital technology within industrial control systems and other components for years. Since 2006, representatives from the U.S. energy sector have been working on a comprehensive strategy for improving the security of cyber systems in the energy sector. The Roadmap to Energy Delivery Systems Cybersecurity[1] presents a vision for developing and maintaining energy delivery systems that could survive an intentional cyber assault. It also outlines a strategic framework for improving cyber security in the energy sector by organizing current efforts and guiding future investments within government and industry. The Roadmap was developed and updated through a collaborative process led by energy asset owners and operators and funded by the Department of Energy (DOE) Office of Electric Delivery and Energy Reliability (OE) in collaboration with the Department of Homeland Security (DHS) Science and Technology Directorate and the Energy Infrastructure Protection Division of Natural Resources Canada.

   What is the Department of Energy doing on this front and how are you working with DOE?

   DOE and industry primarily collaborate in this area through the Cybersecurity for Energy Delivery Systems[2] (CEDS) research and development (R&D) program to develop new cybersecurity solutions in partnership with universities and the national laboratories. This program, run by DOE OE, assists energy sector asset owners and operators by co-funding projects that help detect, prevent, and mitigate the consequences of a cyber incident. Many of the on-going research projects at the National Laboratories involve electricity sector utilities and vendor partners.

[1] https://www.controlsystemsroadmap.net
[2] https://energy.gov/oe/cybersecurity-research-development-and-demonstration-rdd-energy-delivery-systems

The CEDS R&D Program is aligned with DOE's Grid Modernization Initiative[3] (GMI) and the Grid Modernization Multi-Year Program Plan[4] (MYPP). The MYPP identifies the major challenges and opportunities for modernizing the grid and details the research, development, and deployment activities DOE will focus on over the next five years, including opportunities for public-private partnerships. The Electricity Subsector Coordinating Council (ESCC), through its R&D Committee, is working very closely with DOE on this and has identified a number of priorities for collaboration and coordination.

As part of the GMI, DOE announced funding of up to $220 million over three years for the National Labs and partners in January 2016. Funding for the Grid Modernization Laboratory Consortium (GMLC) will support R&D in a number of other key grid modernization areas, such as clean energy integration, standards and test procedures, and advanced storage systems. Many of these projects include electricity sector partners such as utilities, regional transmission organizations and independent system operators, electricity research institutes, and vendors.

What is NERC doing, what is the industry doing, to encourage development and procurement of so-called security by design control systems – those designed to be more invulnerable to cyberattacks?

The industry has been engaged in a number of efforts to encourage development and procurement of energy delivery systems, including the 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity and the 2014 Cybersecurity Procurement Language for Energy Delivery Systems.[5] In 2015, EEI published Principles and Resources for Managing Supply Chain Cybersecurity Risk[6]. Industry is currently working with the North American Electric Reliability Corporation (NERC) to develop a supply chain cybersecurity risk management reliability standard, which will become mandatory upon approval by the Federal Energy Regulatory Commission (FERC). This reliability standard will focus on procurement and operational controls to minimize the risks introduced by industrial control system vendors and their products and services to the bulk-power system. The supply chain cybersecurity risk management standard will be the eleventh mandatory (i.e., regulatory) reliability standard focused on securing industrial control systems used in the bulk-power system.

What is the state of research on this front?

Research in this area is continuing. Adversary tactics are changing and adapting, so it is important for ongoing research to address emerging risks. The Electric Power Research Institute (EPRI) is performing research in this space and is an important partner in

[3] https://energy.gov/under-secretary-science-and-energy/grid-modernization-initiative
[4] https://energy.gov/sites/prod/files/2016/01/f28/Grid%20Modernization%20Multi-Year%20Program%20Plan.pdf
[5] https://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014
[6] http://www.eei.org/issuesandpolicy/testimony-filings-briefs/Documents/150917FinalEEIPrinciplesandResourcesforManagingSupplyChainCybersecurityRisk.pdf

developing risk mitigation strategies.[7] Today there are 128 public-private efforts working to achieve the 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity milestones. **What are the barriers to deployment?**

One of the major barriers to deployment is the typical life cycle of industrial control system components. These devices are typically in service for 10 to 15 years or more. They represent a significant financial investment, and operators of such equipment have limited opportunities to make changes to the components once they are in service, because of the need to maintain high levels of reliability and availability.

2. **While smart or connected technologies offer tremendous opportunities to improve the operation, maintenance and flexibility of electricity systems, they also introduce new potential targets for adversaries or bad actors. This challenge is compounded as more of these connected devices are integrated into the grid and begin to interact with one another and/or other grid networks or services. For example, even if an individual product has strong security, its interaction with other devices or services may introduce a vulnerability. Therefore, understanding threats to the smart grid may require systems level testing to understand how different components interact.**

   What is the industry doing to examine or understand threats to the smart grid, not just at the product level but also from a systems perspective?

   A number of research projects have been launched to understand threats and potential failure modes related to smart grid deployment. In particular, EPRI in partnership with DOE has developed Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology.[8] Industry is also participating in the university-led Cyber Resilient Energy Delivery Consortium (CREDC), which includes the development and deployment of advanced capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes.

   Are DOE or other federal agencies assisting in this research? If so, please elaborate.

   As identified earlier, DOE, the National Labs, and DHS are engaged in assistance with this research. For example, the CREDC program is funded by DOE and DHS. These agencies are among the 18 federal agencies participating in the Networking and Information Technology Research and Development Program (NITRD). NITRD plans and coordinates federally funded work on advanced information technologies, which includes research to improve resilience against cyber-attacks on computer-based systems that monitor, protect, and control critical infrastructure.[9] In February 2016, the National Science and Technology Council and

[7] http://www.epri.com/Our-Work/Pages/Cyber-Security.aspx

[8] https://energy.gov/sites/prod/files/2014/04/f14/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology.pdf

[9] https://www.nitrd.gov/SUBCOMMITTEE/nitrd_agencies/index.aspx#NITRDAgencies

NITRD released the Federal Cybersecurity Research and Development Strategic Plan to guide federal cybersecurity research and development.[10]

Is this an area where DOE or others could be doing more to understand these complex, system level questions?

Continued research in this area is appropriate. The ESCC is working with DOE and other federal partners to prioritize research efforts.

3. **In your testimony you talked about the "Cyber Mutual Assistance Program."**

   Please describe more fully the state of and scope of this program, as it exists today, what equipment, services and personnel it covers, and what plans are for expanding it.

   Today, the industry's deeply embedded culture of mutual assistance is serving as a model for creating responses to cyber threats to the energy grid. Based on lessons from major destructive cyber incidents overseas, and from exercises in North America, the ESCC recommended the formation of a Cyber Mutual Assistance (CMA) Program. The program is a series of initiatives to develop resource sharing relationships intended to provide surge capacity should a cyber incident exceed the capacity for an individual company to respond. These initiatives are a natural extension of the electric power industry's longstanding approach of sharing critical personnel and equipment when responding to emergencies. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power industry is greatly enhancing its ability to defend and protect against threats and to meet customers' expectations.

   The first CMA initiative is the development of a Pool of industry cyber experts who can provide voluntary assistance to other organizations in the event of a disruption to the energy grid due to a cyber emergency. As the CMA Program develops, additional initiatives will be considered and implemented based on the needs and input of participating entities.

   In order to participate in the CMA Program, each participating entity must sign a Mutual Non-Disclosure and Use of Information Agreement, and also designate a Cyber Mutual Assistance Coordinator (CMA Coordinator).

   A CMA Coordinator is a participant's single point of contact for all matters related to the CMA Program, including the Pool. Each Coordinator is responsible for assessing a participant's cyber resources and responding to other participants' requests for assistance, or making a request for emergency assistance on behalf of a participant. The Coordinator also is responsible for preparing and coordinating internal resources in connection with any assistance a participating entity elects to provide.

   In the event of a cyber emergency, any participant may make a direct request for assistance through its CMA Coordinator to any other CMA Coordinator, or may make a broader request

---

10 https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

to multiple or all CMA Coordinators. In responding to a request for assistance, a participating entity's response is voluntary, intended to be advisory in nature, and provided on a short-term basis. Assistance may include services, personnel, or equipment.

As of March 1, 2017, 88 utilities from across the United States and Canada have joined the Cyber Mutual Assistance (CMA) Program. CMA members include utilities from a variety of industry segments, including government-owned utilities, electric cooperatives, regional and independent system operators, and investor-owned utilities.

In exercises for large scale cyber-incidents and power outages, has the industry identified any statutory or regulatory provisions that may unnecessarily delay the sharing of personnel and equipment from federal emergency resources, including the National Guard or FEMA, that would be necessary to respond to and restore systems? If so, would you please describe them?

Exercises of large scale cyber incidents and power outages have revealed at least two specific impediments to the ability of the federal government to respond to industry requests for assistance, and—in particular—the sharing of personnel and equipment from FEMA and the National Guard.

First, under the Stafford Act, FEMA is very limited in its ability to provide assistance to investor-owned utilities. Investor-owned utilities—EEI's members—deliver the vast majority of electricity to customers across the United States, including to many military bases and other critical facilities. Congress should consider revising the Stafford Act to authorize FEMA to provide the same assistance to investor-owned utilities that it can provide to other types of utilities.

Second, recent exercises have revealed that in responding to electric industry requests for assistance in large scale cyber incidents, significant gaps exist in Department of Defense (DOD) policies, plans and doctrines needed to enable the National Guard and to help meet such requests. Section 1648 of the 2016 National Defense Authorization Act (NDAA) requires DOD to develop a comprehensive plan, and to organize and conduct biennial exercises, to support civil authorities in responding to cyber-attacks. Exercises developed pursuant to Section 1648 should help develop options to fill these gaps. The exercises should also include significant participation by EEI and other components of the electricity subsector to insure that industry perspectives can help inform the development of future policies and plans regarding DOD support for post-cyberattack power restoration.

The Honorable Morgan Griffith

1. **Today, the electric industry works with the DOE, with DHS, with the FBI, and other agencies to share information on threats and intelligence. But there does not appear to be a coordinated way for industry to share or receive information across these agencies, leading to more individualized notices from agencies than may be desirable.**

   How can the federal government ensure better coordination within its own agencies and with the electric industry regarding information on threats and intelligence sharing?

Presidential Policy Directive-21 and the 2015 Fixing America's Surface Transportation (FAST) Act have established DOE as the Sector Specific Agency (SSA) for the Energy sector. In this role, DOE has developed an increasingly trusted partnership with the electricity industry, especially through the ESCC. One of the focuses of this group is threat and intelligence information sharing, primarily through classified briefings. DOE's Office of Intelligence is the primary conduit for the electricity sector to receive government intelligence briefings, and all other government intelligence agencies should share any information relevant to the energy sector in a timely and efficient manner.

One major challenge is the delay in granting security clearances to critical industry personnel. DHS, through the National Protection and Programs Directorate (NPPD) Private Sector Clearance Program, in consultation with DOE, should ensure the availability, in a timely manner, of security clearances needed by the energy sector and other critical infrastructure sectors. Current wait times of over two years for a Secret clearance impedes the ability for DOE and other agencies to share their critical threat and intelligence information with the energy sector. DHS and the Office of Personnel Management (OPM) should develop a program dedicated to private critical infrastructure sectors that contains time limits or other measures to ensure expedited processing of clearance applications. The program should also implement a process for "temporary read-in" for key critical infrastructure personnel on an as-needed basis.

The federal government should also coordinate with state and local fusion centers to provide the critical infrastructure owners and operators with localized intelligence. Fusion centers provide a critical convening role for state and local intelligence, law enforcement, and emergency responders. The ability for cleared individuals in the electricity industry, as well as other critical infrastructure sectors, to visit their local fusion center and receive a classified briefing via secure video-teleconference would expedite significantly the government's ability to share timely information on threats and intelligence. Developing partnerships with the fusion centers would also allow opportunities for the private sector to share their insights and intelligence more easily with government partners.

2. **Some electricity utilities are participating in the Cyber Risk Information Sharing Program, which allows the utilities to send network data for analysis against government sources.**

   How can we expand programs like this to provide a frictionless partnership between the public and private sectors that allows private industry to be more agile in its response and allows the government a level of assurance that the power grid is secure?

   In general, utility representatives have found it challenging to obtain clearances in order to better understand threat actors as well as methods used by those threat actors. By the end of 2016, more than 75 percent of all electricity customers were served by an electric company that has deployed CRISP. Efforts are underway to expand participation in this program even further, including finding ways to address challenges in the cost of participation faced by small utilities with limited resources.

The Honorable Frank Pallone

Mr. Aaronson, in your testimony you discuss the Critical Infrastructure Protection (CIP) Reliability Standards, which include both cyber and physical security requirements. These standards are developed and enforced by NERC under the oversight of FERC. Currently, standards for the electric power sector are set by CIP Version 6. In fact, you testified that entities found in violation of CIP standards can face penalties exceeding an astounding $1 million per violation per day.

1. **In 2016, roughly how many entities were in violation of the CIP standards, and roughly how many of these violations were specifically related to non-compliance associated with mandatory protections for cybersecurity?**

   EEI does not collect or track information on CIP standards violations. EEI would defer to NERC on this question, as NERC maintains this information.

2. **I'm also interested in how effective the current version of CIP standards are in mitigating the risks to utilities posed by cyber attackers. Are you aware of any utilities in full compliance with CIP standards that have suffered any breach in their cybersecurity systems? And if so, what lessons can be learned as to how the CIP standards should be strengthened to better improve the cybersecurity protection they provide to utilities?**

   The existing CIP regulations provide a strong baseline level of security. They are the basic "blocking and tackling" measures, the good hygiene. However, we have learned that while these regulations play an important role in strengthening the industry's security posture, regulations alone are insufficient because the threat environment is constantly changing. Threat actors learn and adapt continually. As indicated above, EEI does not collect information regarding CIP standards breaches or compliance, nor are we aware of any such situations. However, NERC and FERC continually review threats, vulnerabilities, and lessons learned from breaches in other countries and industries to help determine whether there are gaps in the CIP standards. Currently, the CIP standards are being modified by two standard drafting teams to address risks identified by the Commission.

   Modifying the CIP standards is a regulatory process that relies on consensus, and most importantly, requires industry expertise to make sure the changes do not create unintended consequences to the operation of the bulk-power system. As a result, modification of these standards takes time to develop, review, and approve. Recognizing the inherently deliberative nature of the standards development and regulatory processes, the industry works closely with its government partners through the ESCC to quickly identify and mitigate new cybersecurity and other risks to the electricity subsector.

   The ESCC is a CEO-level group that is focused on several key areas, including planning and exercising coordinated responses to grid attacks, ensuring that threat information is communicated quickly among government and industry stakeholders, deploying government technologies on utility systems that improve situational awareness of threats to the grid, and cross-sector coordination with other critical infrastructure sectors. These collaborative

industry and government efforts provide timely and effective ways to address evolving threats and vulnerabilities that complement and supplement the CIP standards.

3. **For entities that are non-compliant with CIP standards, what resources are currently available to support capital investments to improve their cybersecurity? What more can be done to motivate utilities to proactively improve and security their cyberinfrastructure?**

   Cost-recovery, primarily through regulatory policies, is always important to support capital investments in the electric sector. This includes investments to maintain compliance with the CIP standards, especially as they are modified.

   Liability protections for investing in cybersecurity tools can also serve as a helpful incentive. For instance, EEI supports clarification that legal liability protections available under the Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002 can be invoked in case of cyber incidents. The DHS SAFETY Act program encourages the development and deployment of effective anti-terrorism products and services, including cyber protections, that utilities and other businesses want to invest in.

   According to the Institute of Electrical and Electronics Engineers, there are a million unfilled cybersecurity engineering jobs around the world, with that number expected to grow to 1.5 million by 2019. In the U.S., there are only 67 job seekers for every 100 open cybersecurity positions.

   So, I'm wondering if this shortage of available workers is posing problems for electric companies seeking cybersecurity experts to fill jobs protecting the security of the electricity grid.

4. **Mr. Aaronson, can you talk about the current situation in the electricity sector as it relates to cybersecurity jobs? Is it indeed true that companies are finding it difficult to hire skilled workers to fill these positions?**

   EEI does not collect or maintain statistics on cybersecurity hiring by our members. But based on regular communications with our members, it is our understanding that many companies are finding it difficult to hire enough skilled workers. The current focus on cyber security by businesses and organizations throughout the United States has created additional demand for individuals with cybersecurity expertise.

5. **In your opinion, would additional federal worker training programs be helpful in boosting qualified candidates in this field?**

   We believe that federal worker training programs could be helpful.

6. **What other role can the federal government play in ensuring we have a robust cybersecurity workforce here in the United States?**

One suggestion would be programs to assist military personnel who may transitioning out of active duty to move into critical infrastructure sectors such as electricity, and to do so in a manner that would allow them to retain existing security clearances.

The Honorable John Sarbanes

1. **What technical or funding support are you receiving from federal agencies on grid cyber security in terms of research and development and standard setting guidance? How could this support be enhanced or improved?**

   EEI does not receive any direct funding from federal agencies for grid security programs. There are a variety of research and development programs in place at DOE and DHS that benefit our sector, however. For example, some EEI members may receive federal funding through participation in DOE CEDS industry partnerships to enhance the reliability and resilience of the nation's energy infrastructure through innovative RD&D cybersecurity solutions.

The Honorable Jerry McNerney

1. **The second installment of the QER noted that the traditional definition of reliability may be insufficient to ensure system integrity and available electric power in the face of physical attacks and cyber threats, among other things. And that the security of the system, particularly cybersecurity, is a growing concern. Would you agree with this assessment?**

   We agree that the threat landscape has changed, particularly with regards to cybersecurity. To some degree, utilities are now expected to defend their systems from nation states or other state-sponsored actors, which has traditionally been the federal government's role. Yet this is now becoming, in effect, a regulatory expectation. The industry is subject to mandatory and enforceable CIP standards that address both cyber and physical security. However, as cyber threats continue to evolve, the regulatory process by nature cannot keep pace. To address this challenge, the industry works closely with its government partners through the ESCC to quickly identify and mitigate new cybersecurity and other risks to the electricity subsector.

2. **Is there a uniform definition used in the energy and electricity sector – or at the federal level – of what cyber "secure" or "resilient" means?**

   Currently there is no universal or common agreement on the precise meaning of cyber "secure" or "resilient". The electric industry recognizes that it may not be able to prevent every outage, and is working to continually enhance its ability to rapidly respond and recover. The industry's philosophy is one of risk management, recognizing that every risk cannot always be predicted or eliminated. The industry works with government through mandatory reliability standards as well as the ESCC and other partnerships to identify and mitigate the key risks to the electricity sector. The reliability standards include ten cybersecurity standards and one physical security standard. The industry is working with

NERC to develop an eleventh cybersecurity standard focusing on minimizing supply chain cybersecurity risk.

3. **How costly is it to fund research RD&D for cyber from a utilities perspective? When updating your networks and physical infrastructure, are you able to put in new, more cyber secure equipment in select areas or does it need to be done across the board? Do you feel cyber security and resilient investments are adequately reflected in rate-making cases?**

   Cyber security research and development can be very costly. Many utilities participate in collaborative R&D initiatives in conjunction with EPRI, which is performing research in this space and is an important partner in developing risk mitigation strategies. DOE, especially through the National Labs, can also be a valuable partner, as can other federal agencies, such as DHS or DOD.

4. **Are customers appropriately knowledgeable on cybersecurity? How do we address that shortcoming?**

   It is our sense is that the general population faces significant challenges in maintaining awareness of current and emerging cyber security risk. The cyber threat is constantly evolving, and consequently customers and the general public are unlikely to be appropriately knowledgeable on cybersecurity. Constant communication and continual education on good cyber hygiene practices can help customers—as well as utilities through their own employees—significantly raise their defenses against cyber threats. Practices such as using strong passwords and passphrases, applying software patches, changing default administrative passwords, identifying and reporting phishing attempts, and knowing what devices are active on the network can considerably reduce customers' risk profiles, making them less of a target for cyber-crime and cyber attacks.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

February 23, 2017

Dr. Chris Beck
Chief Scientist and Vice President
for Policy
The Electric Infrastructure Security Council
840 First Street, N.E.
Washington, DC 20002

Dear Dr. Beck:

Thank you for appearing before the Subcommittee on Energy on Wednesday, February 1, 2017, to testify at the hearing entitled "The Electricity Sector's Efforts to Respond to Cybersecurity Threats."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on March 9, 2017. Your responses should be mailed to Will Batson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Will.Batson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Fred Upton
Chairman
Subcommittee on Energy

cc: The Honorable Bobby Rush, Ranking Member, Subcommittee on Energy

Attachment

House Energy and Commerce Committee, Energy Subcommittee

Hearing: "The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

Answers to Questions for the Record

Chris Beck, EIS Council

March 9, 2017

The Honorable Morgan Griffith

1. **Today, the electric industry works with the DOE, with DHS, with the FBI, and other agencies to share information on threats and intelligence. But there does not appear to be a coordinated way for industry to share or receive information across these agencies, leading to more individualized notices from agencies than may be desirable.**
   A. **How can the federal government ensure better coordination within its own agencies and with the electric industry regarding information on threats and intelligence sharing?**

The Electric Subsector Coordinating Council (ESCC) and the Electric Sector Information Sharing and Analysis Center (E-ISAC) are the two important information sharing bodies in the Electric Subsector and work under the auspices of the Department of Homeland Security (DHS), the agency with overall responsibility for critical infrastructure protection under the National Response Framework (NRF) and National Infrastructure Protection Plan (NIPP), and the Department of Energy (DOE), the electric sector-specific agency under the NIPP and the lead agency for Emergency Support Function 12 (ESF-12) under the NRF. Intelligence and threat information gathered by other Federal agencies (FBI and other Intelligence Community agencies) should flow through DHS/DOE to the ESCC and E-ISAC for effective information sharing and dissemination to electric sector utilities.

Some electricity utilities are participating in the Cyber Risk Information Sharing Program, which allows utilities to send network data for analysis against government sources.

   A. **How can we expand programs like this to provide a frictionless partnership between the public and private sectors that allows private industry to be more agile in its response and allows the government a level of assurance that the power grid is secure?**

The key quality of a sound public/private relationship is trust-building. Information sharing itself is not hard, and protecting the information is straightforward, though the possibility of the information being exfiltrated is always present. The biggest hurdles are the private sector feeling unsure that the government will properly protect sensitive information (from FOIA requests, for example) or use the information against them regarding regulatory compliance. The government has trouble providing information to the private sector because government-held information,

especially intelligence information, is often classified, and especially over-classified. A streamlined process for de-classifying information (or at least lowering the classification level) is needed to rapidly provide necessary information to the electric sector.

The Honorable Frank Pallone

Mr. Beck, your organization focuses on Black Sky hazards. From the perspective of a cyberattack, such an event should be viewed as the worst case scenario: large in scope and duration, likely combining physical and cyberattacks to the grid, and potentially spanning across multiple critical infrastructure sectors.

1. Are the current norms and practices for electricity sector workforce training and development sufficient to prepare workers to respond quickly and effectively to the threat of an imminent or ongoing Black Sky attack?

The current norms and practices are good for what they are designed for: small-scale attack, accident, or disaster. Most of the training and practices at the tactical level can be used for a larger-scale attack, but the strategy has to be different for Black Sky events, due to the greatly expanded scope. To cite one example, if a small scale incident caused the power of a city (or even most of a State – think Superstorm Sandy) to go out but did not affect the surrounding area, the response strategy is to evacuate people from the blackout area, and flow resources from the outside into the affected area to restore the power.

If, on the other hand, the entire Eastern Interconnection blacked out, evacuation is not feasible, and there are not enough "outside" resources to flow in to allow restoration. Current workforce training focuses on the correct tactical areas (malware detection and removal, tech platform rebuild, manual workarounds, etc.) but strategically this won't work for a Black Sky event because it won't be possible to flow enough trained technical support personnel in to help, and in a large-scale attack, utilities may be hesitant to flow those resources to others if they are afraid they may be the next target.

2. What more could be done to improve electricity sector workforce training and development to better prepare workers for such event? In particular, can you speak to any efforts that would better promote intra-sector mutual assistance and cooperation across critical infrastructure sectors, both of which you promoted in your testimony?

The key components of the training are mostly adequate, with the one exception being training mutual assistance on utility-specific operational technology (OT) systems, which is currently challenging due to proprietary business and security concerns. ESCC's Cyber Mutual Assistance Program is certainly making progress in this area, but it is very challenging. Within the electricity subsector, pre-event, cross-utility training for direct OT system support is one option. While individual utilities' OT systems vary, there does exist a commonality of hardware and software system architectures that will allow rapid cross-training for mutual assistance. That said, in a large-scale cyberattack on the electric grid, system personnel within the sector will likely be needed to restore their own systems.

Additional trained personnel from outside of the electric subsector could provide a needed 'surge capacity' from other sectors. The approach being developed by EIS Council is the Certified Power Recovery (CPR) Engineering Team concept, wherein technical personnel from outside the electric power sector – but with requisite computer and electrical engineering backgrounds – can be trained and certified (pre-event) to supplement cybersecurity and power system engineering talent within the sector during large-scale emergency response activities. Another important source of external support is the use of State National Guard forces to help respond to utility requests for assistance.

It is certainly concerning that there are apparently not enough qualified applicants to fill the need for cybersecurity jobs in our country. I think this is a critical aspect of the issue that our Committee should evaluate as we continue our oversight of the security of our electric grid.

This is indeed a concern, needing long-term leadership and incentives – from both government and the private sector – to develop and maintain a robust, trained workforce to address this growing challenge.

The Honorable John Sarbanes

1. **What technical or funding support are you receiving from federal agencies on grid cyber security in terms of research and development and standard setting guidance? How could this support be enhance or improved?**

EIS Council is funded almost exclusively through philanthropic grants and does not currently receive any federal funding. That said, EIS Council considers the current standard-setting process for cybersecurity within the electricity subsector (NERC CIP) to be sufficient as a standard. Electric utilities should use and view the standard as a baseline for their protection activities, but must go beyond the standard in the ever-evolving challenge of cyber adversaries – which the standards simply cannot evolve fast enough to stay abreast of.

The Honorable Jerry McNerney

1. **The second installment of the QER noted that the traditional definition of reliability may be insufficient to ensure system integrity and available electric power in the face of physical attacks and cyber threats, among other things. And that the security of the systems, particularly cybersecurity, is a growing concern. Would you agree with this assessment?**

Yes. The challenge is that the standard metrics for reliability used by regulators – especially at the state level – do not effectively address the impact of physical and cyber- attacks, and cost recovery for resilience investments is a hard case to make. Cyberattacks, as discussed at the hearing, are the most rapidly evolving threat: malware continues to become more sophisticated (though so do the defenses against it); proliferation of malware is very easy and rapid; and the "attack surface" grows as more computer-based systems interface with the grid.

2. **Is there a uniform definition used in the energy and electricity sector – or at the federal level – of what cyber "secure" or "resilient" means?**

Mostly 'Yes' for cyber "secure" definition. The NERC Critical Infrastructure Protection (CIP) Cyber standards outline clear compliance guidelines for cybersecurity practices. This approach is necessary and understandable, and it does serve as a baseline for cybersecurity practices across the Bulk Power System. Compliance with the NERC CIP standards is an important component that highlights accepted practices for increasing the cybersecurity of Bulk Power System utilities. Additionally, the NERC CIP should probably be voluntarily followed by the distribution utilities (even though they are not part of the BPS and therefore not under FERC/NERC jurisdiction) because: 1) they present an attack surface to the BPS, and 2) a sudden loss of load would have significant impact on the BPS.

Mostly 'No' for "resilient" definition. While 'resilient' is typically understood to mean "the ability to withstand an assault/injury and rapidly recover", this has not yet been quantified more precisely. The electric power industry, other infrastructure sectors, government (Federal, and State), and interested academic and non-governmental organizations (including EIS Council) are all working to develop and gain consensus for reasonable resilience metrics.

3. **How costly is it to fund research R&D for cyber from a utilities perspective? When updating your networks and physical infrastructure, are you able to put in new, more cyber secure equipment in select areas or does it need to be done across the board? Do you feel that cyber security and resilient investments are adequately reflected in rate-making cases?**

Cybersecurity R&D is not very costly for government or utilities. Certainly the proliferation of cyberattack methods is very cheap, and while those on the defensive are always at a disadvantage, there are cost-effective methods available for protection and resilience, including critical system isolation, clean, rapidly-installable backup systems, and manual workarounds as necessary.

When updating networks, and physical infrastructure, it is certainly possible to target select areas for protection, to ensure minimal, base-level functionality of the system. Across the board protection, if available/affordable is better, which is captured in the defense-in-depth concept.

Currently such investments present a challenge in rate-making cases. Standard reliability metrics and cyber- or physical security standards do not readily transfer to rate-case making, because prevention of an unspecified outage area and duration due to enhanced security measures are speculative, compared to typical actuarial-informed risk analysis of more commonly addressed reliability concerns.

4. **Are customers appropriately knowledgeable on cybersecurity? How do we address that shortcoming?**

No, customers are not appropriately knowledgeable on cybersecurity. This is still a societal blind spot. Public education on cybersecurity is one avenue. But much more importantly, cybersecurity requirements must become a standard practice within the electric sector – as well as government

– when purchasing equipment from vendors. A canonical example is that computer systems, especially purchased in bulk, often have standardized usernames and passwords that must be changed at the discretion of the utility or user. Often this is overlooked. While the initial overhead of device-specific authentication may seem onerous, real security benefits will flow when individual devices are configured for security. Cybersecurity requires a conscious effort to identify risks at all levels of the Grid.

5. **Electricity is one of our most critical infrastructures. And our ability to respond to natural disasters or attacks requires access to electricity. Your testimony touched on power grid restoration and the need for cross-sector planning. First, do you believe there's adequate cross-sector planning as of now? Does the electricity sector have sufficient capability to communicate and respond to emergency situations?**

As of now, No – but improving (for both questions). In the modern economy, multi-level infrastructure interdependencies have become the norm. In this environment, cross-sector planning is essential to allow rational, effective resilience and disaster response. Too often, though, these cross-sector dependencies are not fully recognized, and there exists the assumption that the other supporting infrastructures/businesses will be operational to support response/recovery/restoration activities, without the requisite recognition of the interdependencies. This could – in some cases – be a mutual 'bootstrap' scenario. For example, a gas-fired electric generator needs just-in-time fuel delivery from a pipeline, which relies on electricity to pump the natural gas to the generator. In other cases it might be a question of restoration priorities. A blacked-out electric utility will typically focus on restoration of the most customers served, often referred to as 'meters', in as short a time as possible. One of those 'meters' could be the local water and/or wastewater utility, which in an emergency is much more important to restore than domicile-level electricity.

Communications represent yet another interdependency. Some electric utilities do have their own communications networks and infrastructure. Most rely to a large degree on the well-known commercial provider telecommunications companies, which in turn rely on electricity. Even for those with their own networks and who can therefore communicate internally to speed restoration, challenges would arise when trying to communicate with government and other infrastructure sectors (who do have a legitimate need to know the power restoration status) when trying to coordinate effective response and restoration actions.

6. **There have been an increasing number of new technologies placed onto the grid in the past decade. Protection throughout the supply chain is an area that deserves our attention, and that standards and best practices should be implemented but not overly prescriptive.**

Agree. The supply chain challenges are daunting, but must be addressed. As was mentioned by Gerry Cauley at the hearing, NERC is now looking at supply-chain security guidance for BPS utilities. Certification requirements from product vendors is one key to addressing this complicated problem. A second is to adopt procurement practices that specify systems with only minimal, stripped down, 'white list' programs, functions, and connectivity. For example, critical

systems should not be procured with any extraneous software applications, require two-factor authentication for any access, and require physical access security protocols.

7. **Are there concerns about potential cyber threats from systems that are already in place but we haven't seen an incident from yet?**

Certainly. There is a widely-used saying in cybersecurity circles: "If you're connected, you're infected." Chief security officers recognize that their systems are under near-constant attack, and that their systems are likely already breached – at least at some level. Continuous monitoring, patching, cleaning, and malware quarantine and removal should be standard operations. In addition, 'clean', disconnected backup systems that can be rapidly installed to replace compromised systems, and the ability to isolate critical components from the larger network, are needed to rapidly respond to currently undetected compromises.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

February 23, 2017

Ms. Barbara Sugg
Vice President and Chief Security Officer
Southwest Power Pool
201 Worthen Drive
Little Rock, AR 72223

Dear Ms. Sugg:

Thank you for appearing before the Subcommittee on Energy on Wednesday, February 1, 2017, to testify at the hearing entitled "The Electricity Sector's Efforts to Respond to Cybersecurity Threats."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on March 9, 2017. Your responses should be mailed to Will Batson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Will.Batson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Fred Upton
Chairman
Subcommittee on Energy

cc: The Honorable Bobby Rush, Ranking Member, Subcommittee on Energy

Attachment

SPP Southwest Power Pool

HELPING OUR MEMBERS WORK TOGETHER
TO KEEP THE LIGHTS ON... TODAY AND IN THE FUTURE

March 9, 2017

The Honorable Fred Upton
Chairman, Subcommittee on Energy
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Chairman Upton:

On behalf of the ISO/RTO Council, thank you again for inviting me to testify before the Energy Subcommittee at the hearing entitled "The Electricity Sector's Efforts to Respond to Cybersecurity Threats." In response to the questions received on February 23, 2017, I have prepared the attached response. Please let me know if I can be of any further assistance related to this important subject.

Sincerely,

Barbara Sugg
Vice President of Information Technology, Chief Security Officer
Southwest Power Pool, Inc.
201 Worthen Dr.
Little Rock, AR 72223
501-614-3245 • bsugg@spp.org

cc: The Honorable Bobby Rush, Ranking Member, Subcommittee on Energy

The Honorable Morgan Griffith

1. **Today, the electric industry works with the DOE, with DHS, with the FBI, and other agencies to share information on threats and intelligence. But there does not appear to be a coordinated way for industry to share or receive information across these agencies, leading to more individualized notices from agencies than may be desirable.**

    a. **How can the federal government ensure better coordination within its own agencies and with the electric industry regarding information on threats and intelligence sharing?**

    Instead of the industry receiving information individually from each of these agencies, a suggestion would be for the DOE, DHS and FBI to work directly with the E-ISAC to communicate threat information to the various entities. As the E-ISAC is governed by the E-ISAC Member Executive Committee of the ESCC which is the executive conduit between government agencies and the electric industry we believe that leveraging this existing governance model is an effective way to coordinate between government and industry. This is a similar model to the financial sector and communications sector.

2. **Some electricity utilities are participating in the Cyber Risk Information Sharing Program (CRISP), which allows the utilities to send network data for analysis against government sources.**

    a. **How can we expand programs like this to provide a frictionless partnership between the public and private sectors that allows private industry to be more agile in its response and allows the government a level of assurance that the power grid is secure?**

    While CRISP is a valuable program, it is costly due to the fact that there are only a small number of participants and the entire cost of the program is shared amongst all of its participants. Subsidizing the cost for the government analysis, thus lowering the cost would encourage more entities to join. Please keep in mind that CRISP analysis is shared with the rest of the sector via the E-ISAC.

The Honorable John Sarbanes

1. **What technical or funding support are you receiving from federal agencies on grid cyber security in terms of research and development and standard setting guidance? How could this support be enhanced or improved?**

    While the ISO/RTOs are not receiving direct federal funding support, we are partnering with DOE, DOD, the Defense Advanced Research Projects Agency (DARPA), and other research organizations who are receiving federal funding. In these cases we are providing industry expertise to guide research and development (R&D) investment. Additionally, the Electricity Subsector Coordinating Council R&D committee is working with government and industry focusing on high priority R&D topics: i) impacts of Electromagnetic Pulse (EMP) threats on the Power Grid, ii) enhanced communication capabilities during significant cyber or physical

disruptions, and iii) improved and automated threat information sharing across the electric sector and other critical infrastructure sectors, and iv) advanced automation capabilities to execute efficient response operations.

The Honorable Jerry McNerney

1. **The second installment of the QER noted that the traditional definition of reliability may be insufficient to ensure system integrity and available electric power in the face of physical attacks and cyber threats, among other things. And that the security of the system, particularly cybersecurity, is a growing concern. Would you agree with this assessment?**

   The electric industry has a solid foundation of providing reliable electric service, but certainly the reliability, resiliency, and security of the bulk electric system must be taken into account. There is considerable ongoing discussion in various industry forums such as NERC and the Transmission Forum around resiliency and security, in addition to continuing discussion of traditional reliability issues. For instance, the industry is considering the disruption that can be caused by lower-frequency events (unusually severe weather, physical attacks, cyber threats, etc.) that have a potentially high impact on the electric system, often reflected in additional best practices that should be used in planning and operating systems.

2. **Is there a uniform definition used in the energy and electricity sector – or at the federal level – of what cyber "secure" or "resilient" means?**

   We do not believe there is a uniform definition that has been adopted within the electrical sector. However, Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience attempts to define the terms as:

   Security - Reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

   Resilience - the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

3. **How costly is it to fund research RD&D from a utilities perspective? When updating your networks and physical infrastructure, are you able to put in new, more cyber secure equipment in select areas or does it need to be done across the board? Do you feel that cyber security and resilient investments are adequately reflected in rate-making cases?**

   Networks are typically designed in layers, which allow select areas to be upgraded and/or maintained without having a negative impact on other areas.

   Rate making-cases vary from region to region. Typically rate cases will not specifically identify security, but they implicitly include security requirements. Resilience is a broad term and the future will need to consider investment that improves upon traditional reliability and considers a grid with less critical components and resilience built into the design.

4. **Are customers appropriately knowledgeable on cybersecurity? How do we address that shortcoming?**

ISO/RTOs operate at the wholesale level. Our "customers" are market participants, utility companies and transmission owners, therefore they are reasonably well versed in cybersecurity as they have standards they are required to meet.