NEAL R. GROSS & CO., INC.

RPTS MILLER

HIF032030

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, D.C.

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.

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

Today's hearing -- I recognize myself for five 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 it becomes particularly challenging.

So 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, 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.

But I don't think that anyone will dispute that improvement 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 -- 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 have got to continue to build a record about electric sector efforts to address cyber security threats. This will help us identify whether additional measures are necessary, and 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 in the ongoing efforts.

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.

So 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.

And at this point, I recognize the ranking member of the subcommittee, my friend from Chicago, Mr. Townes. Mr. Rush.

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 security

-- 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 put more -- 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.

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.

Mr. Upton. 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 and so look forward to having that happen.

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

Mr. Walden. Thank you, Mr. Upton.

We --

Mr. Upton. Welcome to your first appearance before the subcommittee as --

Mr. Walden. You know, I am delighted to be here.

Mr. Upton. -- full committee chair.

Mr. Walden. 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's being done to address and respond to the cybersecurity threats to our nation's electricity system.

Now, 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 incident information and communications enabled by digital technology become more essential for our electricity system to operate at increased levels of reliability.

Now, 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's 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.

So this will lay the groundwork for closer scrutiny of the relevant policies necessary to ensure future reliability in this ever 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 you all run that grid test periodically and the tabletopping of it and so we will be interested to hearing 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?

So 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.

Mr. Upton. Thank you. 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, and we'd ask you to summarize it and take about five 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 those of us that served with you. Thank you. Thanks, Bobby.

(Applause.)

Mr. Cauley, you're recognized for five 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; DR. 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 and Committee Chairman Walden and 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 and 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 Gerry W. Cauley follows:]

**********INSERT 1**********

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 sector -- 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 securities -- the industry's security posture.

Failure to comply can cost companies more than a million dollars per infraction per day. So, suffice 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 -- 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 -- 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 spared sharing -- 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 be here and look forward to answering your questions.

[The statement of Scott I. Aaronson follows:]

**********INSERT 2**********

Mr. Upton. Thank you very much.

Dr. Beck.

STATEMENT OF DR. CHRIS BECK

Mr. 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 but 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-attacks threat time line 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 TO 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 are 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 TO 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 sector -- in the electric power sector.

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

[The statement of Dr. Chris Beck follows:]

**********INSERT 3**********

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 committees -- sorry, 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, and 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 opportunities 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 do 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 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 Barbara Sugg follows:]

**********INSERT 4**********

Mr. Upton. Well, thank you all.

I think each of you mentioned that it is a daunting task. I mean, 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 the -- 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 I think 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. So 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 -- a high level of -- set of entities to coordinate with should the unthinkable happen.

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

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

One of the concerns that a number of us have raised that 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 it would 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 -- we run the exercise in a way that's two days -- 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. Now, the results of that are they in a classified setting?

Mr. Cauley. There is a public report for each of the -- for each of the exercises. What we found is that we -- 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 at -- in the past, not just industry but government, like, well, we never thought of it that way.

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

Mr. Upton. And I know my time is expired but let me just -- I have one quick question on that. Were the governors engaged in this -- in the 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 have -- 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 to 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 -- 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 a 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 protects 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 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,

I think, 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 I think 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 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 that that 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 is 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 recognize the chairman of the full committee, Mr. Walden, for five 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 and you were talking about you go out to the substation, you call the FBI, you do all that and we got the call into the radio station to announce that Bonneville Dam, one of the major dams crossing the Columbia River, we were supposed to announce on air had been breached.

Fortunately, I had a sort of retired announcer back working that Saturday morning who said, you know, 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 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 do -- 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 -- reliability of the grid, the threats that are there. We are very cognizant of the cyber security issues. And the attempts by others to put -- perhaps 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 with you in a -- 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 and we can sleep --

Mr. Cauley. Well, I think -- I'll just start the -- 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, you know, 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 is -- 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? It's --

Mr. Cauley. We have not particularly sought after that but I know Dr. Beck and his crew at EIS has had some work around --

Mr. Walden. Yes, because they are often --

Mr. Cauley. -- the use of ham operators for emergencies.

Mr. Walden. Yeah, they are the only communication tool left. But go ahead, Mr. Aaronson.

Mr. Aaronson. So sort of 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 or, you know,

look at Sony, look at Target.

I think 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, you know, 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 -- okay, 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.

Mr. Beck. I would say, going to Scott's point about the social aspect, I would -- I don't see any -- to your question, Chairman Walden, that there is 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 are -- 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 they have a different understanding of it. The CFOs, et cetera, and so we need to -- we need to look at all of those inner -- you know, 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, you know, what's coming out of the government and, you know, what -- 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 and 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 be -- would help reduce the threat of transformer attack or do we need a transformer reserve -- 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, you know, 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 transformers, 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 -- 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 is 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 -- 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 is 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 -- in our training and education from, you know, how to ensure that you don't click on emails you shouldn't click 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 haven't -- we haven't seen incidents yet?

Mr. 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.

So rather than -- 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 -- 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 we -- 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.

But 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 is not -- if it's not connected to the grid it's 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. Upton. Gentleman's time is expired.

The chair calls upon the vice chairman of the full committee, Mr. Barton from Texas, for five 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. -- is it Sugg or Suge?

Ms. Sugg. Sugg.

Mr. Barton. 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, you know, 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 entities -- 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 -- you give him an A?

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

Mr. Barton. Dr. Beck.

Mr. 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. Okay. 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 -- you know, 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 A's. 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 and I think --

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

Mr. Cauley. Something along those lines. But -- and 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 we -- 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. Okay. 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 five 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, that the -- 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 do we need to do to make sure -- 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, much like -- 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 -- 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, you know, maybe a military micro grid has better protections than the average household device.

But I am thinking, you know, now you have these home devices. You turn energy on and off. I assume that that is a point of vulnerability and how do you -- how do -- what do we do to make sure that the security you talked about is, as you said, baked in? What is it -- what is it that we need to do? Is it standards or is it -- what would it be?

Mr. Aaronson. I think it is standards and requirements. When you talk about -- 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 -- they have -- they are being put out at the -- I think the number is 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.

Mr. Beck. I would just add that, again, it's also to the -- to 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. I mean, why would they care about the larger grid? What is going to be incentive for an individual customer to talk about that?

Mr. 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 -- 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 -- 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. Upton. Gentleman yields back.

The chair calls upon himself for five 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 emails of employees are standard format, first name dot last name dot organization dot com, dot org, something like that.

Got those, put attachment 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 an officer for -- a

pilot for nine years. They teach us 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 including -- and then also 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, I believe, is what that stands for, 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 know what was going on.

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

Mr. Upton. 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 just so -- 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, you know, 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. Upton. 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. Upton. Good. Dr. Beck, add anything to those line of questioning?

Mr. 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, right, you don't disturb the scene. You rope it off and then you analyze it and try to figure out what happened while -- but that crime scene is a broken down system that the operators want to restore.

They don't -- they don't want to leave a mess that

people can look through. So they're -- 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 that we -- and that we don't know where all it is embedded.

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

Mr. Beck. I would say, commensurate with the -- with the incoming administration's emphasis on infrastructure that leadership be shown there, that -- 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 -- as it is upgraded, not -- we can't be introducing or reintroducing old vulnerabilities or introducing new ones.

Mr. Upton. 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. Upton. 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 five minutes and he has departed so I guess it's going to be Ms. Castor from Florida for five 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. Okay. 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 --

Ms. Castor. Exactly, because of --

Mr. Cauley. -- opening a -- 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 six months prior to the main attack.

These included emails 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. So there -- what was not -- 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 of the security -- all of the security facets of this.

And 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. Upton. The gentlelady's time has expired.

The chair calls upon the gentleman from Pennsylvania,

Mr. Murphy, for five minutes.

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

A couple things -- 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 am going back to -- 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 --

Mr. Beck. That was Target.

Mr. Murphy. Oh, it was Target? Okay. 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 with -- 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 a unsavvy vendor, whether it is even a savvy user, you know, 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 of, 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 potential -- 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 with about -- within about six 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, you know, 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 -- 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. I am not sure if that gets to --

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

One of the -- 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 we are -- are we creating more inefficiencies in our system.

Dr. Beck, go ahead.

Mr. Beck. Well, it's still a challenge. So I talked about the silos before. But I would say no but it is improving. But those -- 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.

Mr. 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 if -- with leadership and they -- and they end up working on similar problems and find out later wow, you know, we have a, you know, a military application -- we had a problem here but 90 percent of that problem might be relevant for a civilian electric power grid.

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

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

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

Mr. Tonko. Thank you, Mr. Chair.

Welcome to our panelists. The -- 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. Okay. 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 cyber-attack.

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 actually -- is the right information or has not been compromised in some way. So we are -- 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. Okay. Dr. Beck, did you want to say something?

Mr. Beck. I would say I largely agree with that but, again, with particular respect to cybersecurity, there are

additional challenges to expanding the -- expanding mutual assistance, which the industry has a long history of.

When it's -- 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 TO 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 just a -- it's a resource challenge. I applause ESCC for taking it up.

But it is -- 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 -- that it is in its nascent stages and mutual assistance in its traditional form grew up under the crucible of lots and lots of -- or 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 going to leverage those -- it 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 complement 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. Upton. Gentleman's time has expired. The chair calls upon the gentleman from Mississippi, Mr. Harper, for five 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 is a -- there is much more devices -- 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. Okay. 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 out -- 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 is 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. Upton. The gentleman from Maryland, Mr. Sarbanes, for five minutes.

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

I am trying to get my head around how much of the grid is -- 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. Yeah.

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.

NERC -- 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, you know, 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 -- is it feasible to think in terms of, like, 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.

If you can -- 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, you know, sometimes the

frailty is a human being enables something to get through. But so we are doing that.

I think we have a really -- 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 -- 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 sort 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 we simply -- instead of -- instead of trying to fully cordon off I think the most -- you know, the most critical assets I think 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 -- to the promulgation of distributed resources are -- it's going in the right direction.

Mr. Sarbanes. I yield back. Thanks.

Mr. Upton. The gentleman yields back. The chair calls upon the gentleman from West Virginia, Mr. McKinley, for five 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 six 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 Tom said -- 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 a ongoing effort to continue to improve our defenses to respond to incidents

internationally and domestically and to apply those here. You know, you have two options.

You can be -- 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 roundtable -- a 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 okay. They are saying from the inside we are not.

So I am still going to remain uncomfortable -- that I think it's -- 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 -- 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.

Mr. 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 that the -- 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 website.

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 we -- periodically we get briefed on different terrorism attacks.

If 56 were stopped last month or whatever that -- 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. Upton. Gentleman yields back.

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

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

Mr. Aaronson, for you first -- you know, 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 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 four 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. Okay. Good. Well, thank you for that. Anybody else want to comment on that? I've got a couple of other questions. Okay.

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 the -- one of capabilities we have through CRISP and through our analytics is to see patterns of connection points of adversary -- internet locations, signatures of compromise and things like that.

We can see a pattern over three months, six 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. Okay.

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.

Mr. 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 know that -- to have visibility to those reports to understand, like, you know, this situation is happening or the frequency of attacks or, you know, that people are reporting it I think that just raises the consciousness of keeping your eye on this particular ball.

Mr. Johnson. Okay. 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 need -- 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. Okay. Great. Mr. Chairman, I yield

back. Thanks for indulging.

Mr. Upton. Gentleman yields back. The chair calls upon the gentleman from Michigan, Mr. Walberg, for five 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, the Canadian -- 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 customers 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. Upton. The gentleman yields back.

We saved the best for last. The chair calls upon the gentleman from Ohio, Mr. Latta, for five 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. Okay. 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 -- 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, yeah, we are secure, we would not be able to be responsive to new and emerging threats.

So, you know, 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 the -- 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. Upton. 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 the Super Bowl -- Super Bowl 51. It's not 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. So 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.

Without objection, the Subcommittee is adjourned.

[Whereupon, at 12:49 p.m., the Subcommittee was

adjourned.]