Responses from Scott L. Aaronson
Edison Electric Institute

Subcommittee on Energy Hearing
"The Electricity Sector's Efforts to Respond to Cybersecurity Threats"
February 1, 2017

Additional Questions for the Record

The Honorable Fred Upton

1. **One of the challenges the electric sector faces appears to stem from harnessing digital technology onto industrial control systems and other components that were not designed to account for the risks modern malware and digital communications may create.**

   Explain how NERC and industry are working to develop policies to encourage development of system components that will be less vulnerable to attack?

   The industry has been focused on managing and reducing risk associated with the use of digital technology within industrial control systems and other components for years. Since 2006, representatives from the U.S. energy sector have been working on a comprehensive strategy for improving the security of cyber systems in the energy sector. The Roadmap to Energy Delivery Systems Cybersecurity[1] presents a vision for developing and maintaining energy delivery systems that could survive an intentional cyber assault. It also outlines a strategic framework for improving cyber security in the energy sector by organizing current efforts and guiding future investments within government and industry. The Roadmap was developed and updated through a collaborative process led by energy asset owners and operators and funded by the Department of Energy (DOE) Office of Electric Delivery and Energy Reliability (OE) in collaboration with the Department of Homeland Security (DHS) Science and Technology Directorate and the Energy Infrastructure Protection Division of Natural Resources Canada.

   What is the Department of Energy doing on this front and how are you working with DOE?

   DOE and industry primarily collaborate in this area through the Cybersecurity for Energy Delivery Systems[2] (CEDS) research and development (R&D) program to develop new cybersecurity solutions in partnership with universities and the national laboratories. This program, run by DOE OE, assists energy sector asset owners and operators by co-funding projects that help detect, prevent, and mitigate the consequences of a cyber incident. Many of the on-going research projects at the National Laboratories involve electricity sector utilities and vendor partners.

[1] https://www.controlsystemsroadmap.net
[2] https://energy.gov/oe/cybersecurity-research-development-and-demonstration-rdd-energy-delivery-systems

The CEDS R&D Program is aligned with DOE's Grid Modernization Initiative[3] (GMI) and the Grid Modernization Multi-Year Program Plan[4] (MYPP). The MYPP identifies the major challenges and opportunities for modernizing the grid and details the research, development, and deployment activities DOE will focus on over the next five years, including opportunities for public-private partnerships. The Electricity Subsector Coordinating Council (ESCC), through its R&D Committee, is working very closely with DOE on this and has identified a number of priorities for collaboration and coordination.

As part of the GMI, DOE announced funding of up to $220 million over three years for the National Labs and partners in January 2016. Funding for the Grid Modernization Laboratory Consortium (GMLC) will support R&D in a number of other key grid modernization areas, such as clean energy integration, standards and test procedures, and advanced storage systems. Many of these projects include electricity sector partners such as utilities, regional transmission organizations and independent system operators, electricity research institutes, and vendors.

What is NERC doing, what is the industry doing, to encourage development and procurement of so-called security by design control systems – those designed to be more invulnerable to cyberattacks?

The industry has been engaged in a number of efforts to encourage development and procurement of energy delivery systems, including the 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity and the 2014 Cybersecurity Procurement Language for Energy Delivery Systems.[5] In 2015, EEI published Principles and Resources for Managing Supply Chain Cybersecurity Risk[6]. Industry is currently working with the North American Electric Reliability Corporation (NERC) to develop a supply chain cybersecurity risk management reliability standard, which will become mandatory upon approval by the Federal Energy Regulatory Commission (FERC). This reliability standard will focus on procurement and operational controls to minimize the risks introduced by industrial control system vendors and their products and services to the bulk-power system. The supply chain cybersecurity risk management standard will be the eleventh mandatory (i.e., regulatory) reliability standard focused on securing industrial control systems used in the bulk-power system.

What is the state of research on this front?

Research in this area is continuing. Adversary tactics are changing and adapting, so it is important for ongoing research to address emerging risks. The Electric Power Research Institute (EPRI) is performing research in this space and is an important partner in

[3] https://energy.gov/under-secretary-science-and-energy/grid-modernization-initiative
[4] https://energy.gov/sites/prod/files/2016/01/f28/Grid%20Modernization%20Multi-Year%20Program%20Plan.pdf
[5] https://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014
[6] http://www.eei.org/issuesandpolicy/testimony-filings-briefs/Documents/150917FinalEEIPrinciplesandResourcesforManagingSupplyChainCybersecurityRisk.pdf

developing risk mitigation strategies.[7] Today there are 128 public-private efforts working to achieve the 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity milestones. **What are the barriers to deployment?**

One of the major barriers to deployment is the typical life cycle of industrial control system components. These devices are typically in service for 10 to 15 years or more. They represent a significant financial investment, and operators of such equipment have limited opportunities to make changes to the components once they are in service, because of the need to maintain high levels of reliability and availability.

2. **While smart or connected technologies offer tremendous opportunities to improve the operation, maintenance and flexibility of electricity systems, they also introduce new potential targets for adversaries or bad actors. This challenge is compounded as more of these connected devices are integrated into the grid and begin to interact with one another and/or other grid networks or services. For example, even if an individual product has strong security, its interaction with other devices or services may introduce a vulnerability. Therefore, understanding threats to the smart grid may require systems level testing to understand how different components interact.**

   What is the industry doing to examine or understand threats to the smart grid, not just at the product level but also from a systems perspective?

   A number of research projects have been launched to understand threats and potential failure modes related to smart grid deployment. In particular, EPRI in partnership with DOE has developed Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology.[8] Industry is also participating in the university-led Cyber Resilient Energy Delivery Consortium (CREDC), which includes the development and deployment of advanced capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes.

   Are DOE or other federal agencies assisting in this research? If so, please elaborate.

   As identified earlier, DOE, the National Labs, and DHS are engaged in assistance with this research. For example, the CREDC program is funded by DOE and DHS. These agencies are among the 18 federal agencies participating in the Networking and Information Technology Research and Development Program (NITRD). NITRD plans and coordinates federally funded work on advanced information technologies, which includes research to improve resilience against cyber-attacks on computer-based systems that monitor, protect, and control critical infrastructure.[9] In February 2016, the National Science and Technology Council and

[7] http://www.epri.com/Our-Work/Pages/Cyber-Security.aspx

[8] https://energy.gov/sites/prod/files/2014/04/f14/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology.pdf

[9] https://www.nitrd.gov/SUBCOMMITTEE/nitrd_agencies/index.aspx#NITRDAgencies

NITRD released the Federal Cybersecurity Research and Development Strategic Plan to guide federal cybersecurity research and development.[10]

Is this an area where DOE or others could be doing more to understand these complex, system level questions?

Continued research in this area is appropriate. The ESCC is working with DOE and other federal partners to prioritize research efforts.

3. In your testimony you talked about the "Cyber Mutual Assistance Program."

Please describe more fully the state of and scope of this program, as it exists today, what equipment, services and personnel it covers, and what plans are for expanding it.

Today, the industry's deeply embedded culture of mutual assistance is serving as a model for creating responses to cyber threats to the energy grid. Based on lessons from major destructive cyber incidents overseas, and from exercises in North America, the ESCC recommended the formation of a Cyber Mutual Assistance (CMA) Program. The program is a series of initiatives to develop resource sharing relationships intended to provide surge capacity should a cyber incident exceed the capacity for an individual company to respond. These initiatives are a natural extension of the electric power industry's longstanding approach of sharing critical personnel and equipment when responding to emergencies. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power industry is greatly enhancing its ability to defend and protect against threats and to meet customers' expectations.

The first CMA initiative is the development of a Pool of industry cyber experts who can provide voluntary assistance to other organizations in the event of a disruption to the energy grid due to a cyber emergency. As the CMA Program develops, additional initiatives will be considered and implemented based on the needs and input of participating entities.

In order to participate in the CMA Program, each participating entity must sign a Mutual Non-Disclosure and Use of Information Agreement, and also designate a Cyber Mutual Assistance Coordinator (CMA Coordinator).

A CMA Coordinator is a participant's single point of contact for all matters related to the CMA Program, including the Pool. Each Coordinator is responsible for assessing a participant's cyber resources and responding to other participants' requests for assistance, or making a request for emergency assistance on behalf of a participant. The Coordinator also is responsible for preparing and coordinating internal resources in connection with any assistance a participating entity elects to provide.

In the event of a cyber emergency, any participant may make a direct request for assistance through its CMA Coordinator to any other CMA Coordinator, or may make a broader request

[10] https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

to multiple or all CMA Coordinators. In responding to a request for assistance, a participating entity's response is voluntary, intended to be advisory in nature, and provided on a short-term basis. Assistance may include services, personnel, or equipment.

As of March 1, 2017, 88 utilities from across the United States and Canada have joined the Cyber Mutual Assistance (CMA) Program. CMA members include utilities from a variety of industry segments, including government-owned utilities, electric cooperatives, regional and independent system operators, and investor-owned utilities.

In exercises for large scale cyber-incidents and power outages, has the industry identified any statutory or regulatory provisions that may unnecessarily delay the sharing of personnel and equipment from federal emergency resources, including the National Guard or FEMA, that would be necessary to respond to and restore systems? If so, would you please describe them?

Exercises of large scale cyber incidents and power outages have revealed at least two specific impediments to the ability of the federal government to respond to industry requests for assistance, and—in particular—the sharing of personnel and equipment from FEMA and the National Guard.

First, under the Stafford Act, FEMA is very limited in its ability to provide assistance to investor-owned utilities. Investor-owned utilities—EEI's members—deliver the vast majority of electricity to customers across the United States, including to many military bases and other critical facilities. Congress should consider revising the Stafford Act to authorize FEMA to provide the same assistance to investor-owned utilities that it can provide to other types of utilities.

Second, recent exercises have revealed that in responding to electric industry requests for assistance in large scale cyber incidents, significant gaps exist in Department of Defense (DOD) policies, plans and doctrines needed to enable the National Guard and to help meet such requests. Section 1648 of the 2016 National Defense Authorization Act (NDAA) requires DOD to develop a comprehensive plan, and to organize and conduct biennial exercises, to support civil authorities in responding to cyber-attacks. Exercises developed pursuant to Section 1648 should help develop options to fill these gaps. The exercises should also include significant participation by EEI and other components of the electricity subsector to insure that industry perspectives can help inform the development of future policies and plans regarding DOD support for post-cyberattack power restoration.

The Honorable Morgan Griffith

1. **Today, the electric industry works with the DOE, with DHS, with the FBI, and other agencies to share information on threats and intelligence. But there does not appear to be a coordinated way for industry to share or receive information across these agencies, leading to more individualized notices from agencies than may be desirable.**

   How can the federal government ensure better coordination within its own agencies and with the electric industry regarding information on threats and intelligence sharing?

Presidential Policy Directive-21 and the 2015 Fixing America's Surface Transportation (FAST) Act have established DOE as the Sector Specific Agency (SSA) for the Energy sector. In this role, DOE has developed an increasingly trusted partnership with the electricity industry, especially through the ESCC. One of the focuses of this group is threat and intelligence information sharing, primarily through classified briefings. DOE's Office of Intelligence is the primary conduit for the electricity sector to receive government intelligence briefings, and all other government intelligence agencies should share any information relevant to the energy sector in a timely and efficient manner.

One major challenge is the delay in granting security clearances to critical industry personnel. DHS, through the National Protection and Programs Directorate (NPPD) Private Sector Clearance Program, in consultation with DOE, should ensure the availability, in a timely manner, of security clearances needed by the energy sector and other critical infrastructure sectors. Current wait times of over two years for a Secret clearance impedes the ability for DOE and other agencies to share their critical threat and intelligence information with the energy sector. DHS and the Office of Personnel Management (OPM) should develop a program dedicated to private critical infrastructure sectors that contains time limits or other measures to ensure expedited processing of clearance applications. The program should also implement a process for "temporary read-in" for key critical infrastructure personnel on an as-needed basis.

The federal government should also coordinate with state and local fusion centers to provide the critical infrastructure owners and operators with localized intelligence. Fusion centers provide a critical convening role for state and local intelligence, law enforcement, and emergency responders. The ability for cleared individuals in the electricity industry, as well as other critical infrastructure sectors, to visit their local fusion center and receive a classified briefing via secure video-teleconference would expedite significantly the government's ability to share timely information on threats and intelligence. Developing partnerships with the fusion centers would also allow opportunities for the private sector to share their insights and intelligence more easily with government partners.

2. **Some electricity utilities are participating in the Cyber Risk Information Sharing Program, which allows the utilities to send network data for analysis against government sources.**

   How can we expand programs like this to provide a frictionless partnership between the public and private sectors that allows private industry to be more agile in its response and allows the government a level of assurance that the power grid is secure?

   In general, utility representatives have found it challenging to obtain clearances in order to better understand threat actors as well as methods used by those threat actors. By the end of 2016, more than 75 percent of all electricity customers were served by an electric company that has deployed CRISP. Efforts are underway to expand participation in this program even further, including finding ways to address challenges in the cost of participation faced by small utilities with limited resources.

The Honorable Frank Pallone

Mr. Aaronson, in your testimony you discuss the Critical Infrastructure Protection (CIP) Reliability Standards, which include both cyber and physical security requirements. These standards are developed and enforced by NERC under the oversight of FERC. Currently, standards for the electric power sector are set by CIP Version 6. In fact, you testified that entities found in violation of CIP standards can face penalties exceeding an astounding $1 million per violation per day.

1. **In 2016, roughly how many entities were in violation of the CIP standards, and roughly how many of these violations were specifically related to non-compliance associated with mandatory protections for cybersecurity?**

   EEI does not collect or track information on CIP standards violations. EEI would defer to NERC on this question, as NERC maintains this information.

2. **I'm also interested in how effective the current version of CIP standards are in mitigating the risks to utilities posed by cyber attackers. Are you aware of any utilities in full compliance with CIP standards that have suffered any breach in their cybersecurity systems? And if so, what lessons can be learned as to how the CIP standards should be strengthened to better improve the cybersecurity protection they provide to utilities?**

   The existing CIP regulations provide a strong baseline level of security. They are the basic "blocking and tackling" measures, the good hygiene. However, we have learned that while these regulations play an important role in strengthening the industry's security posture, regulations alone are insufficient because the threat environment is constantly changing. Threat actors learn and adapt continually. As indicated above, EEI does not collect information regarding CIP standards breaches or compliance, nor are we aware of any such situations. However, NERC and FERC continually review threats, vulnerabilities, and lessons learned from breaches in other countries and industries to help determine whether there are gaps in the CIP standards. Currently, the CIP standards are being modified by two standard drafting teams to address risks identified by the Commission.

   Modifying the CIP standards is a regulatory process that relies on consensus, and most importantly, requires industry expertise to make sure the changes do not create unintended consequences to the operation of the bulk-power system. As a result, modification of these standards takes time to develop, review, and approve. Recognizing the inherently deliberative nature of the standards development and regulatory processes, the industry works closely with its government partners through the ESCC to quickly identify and mitigate new cybersecurity and other risks to the electricity subsector.

   The ESCC is a CEO-level group that is focused on several key areas, including planning and exercising coordinated responses to grid attacks, ensuring that threat information is communicated quickly among government and industry stakeholders, deploying government technologies on utility systems that improve situational awareness of threats to the grid, and cross-sector coordination with other critical infrastructure sectors. These collaborative

industry and government efforts provide timely and effective ways to address evolving threats and vulnerabilities that complement and supplement the CIP standards.

3. **For entities that are non-compliant with CIP standards, what resources are currently available to support capital investments to improve their cybersecurity? What more can be done to motivate utilities to proactively improve and security their cyberinfrastructure?**

   Cost-recovery, primarily through regulatory policies, is always important to support capital investments in the electric sector. This includes investments to maintain compliance with the CIP standards, especially as they are modified.

   Liability protections for investing in cybersecurity tools can also serve as a helpful incentive. For instance, EEI supports clarification that legal liability protections available under the Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002 can be invoked in case of cyber incidents. The DHS SAFETY Act program encourages the development and deployment of effective anti-terrorism products and services, including cyber protections, that utilities and other businesses want to invest in.

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

   So, I'm wondering if this shortage of available workers is posing problems for electric companies seeking cybersecurity experts to fill jobs protecting the security of the electricity grid.

4. **Mr. Aaronson, can you talk about the current situation in the electricity sector as it relates to cybersecurity jobs? Is it indeed true that companies are finding it difficult to hire skilled workers to fill these positions?**

   EEI does not collect or maintain statistics on cybersecurity hiring by our members. But based on regular communications with our members, it is our understanding that many companies are finding it difficult to hire enough skilled workers. The current focus on cyber security by businesses and organizations throughout the United States has created additional demand for individuals with cybersecurity expertise.

5. **In your opinion, would additional federal worker training programs be helpful in boosting qualified candidates in this field?**

   We believe that federal worker training programs could be helpful.

6. **What other role can the federal government play in ensuring we have a robust cybersecurity workforce here in the United States?**

One suggestion would be programs to assist military personnel who may transitioning out of active duty to move into critical infrastructure sectors such as electricity, and to do so in a manner that would allow them to retain existing security clearances.

The Honorable John Sarbanes

1. **What technical or funding support are you receiving from federal agencies on grid cyber security in terms of research and development and standard setting guidance? How could this support be enhanced or improved?**

   EEI does not receive any direct funding from federal agencies for grid security programs. There are a variety of research and development programs in place at DOE and DHS that benefit our sector, however. For example, some EEI members may receive federal funding through participation in DOE CEDS industry partnerships to enhance the reliability and resilience of the nation's energy infrastructure through innovative RD&D cybersecurity solutions.

The Honorable Jerry McNerney

1. **The second installment of the QER noted that the traditional definition of reliability may be insufficient to ensure system integrity and available electric power in the face of physical attacks and cyber threats, among other things. And that the security of the system, particularly cybersecurity, is a growing concern. Would you agree with this assessment?**

   We agree that the threat landscape has changed, particularly with regards to cybersecurity. To some degree, utilities are now expected to defend their systems from nation states or other state-sponsored actors, which has traditionally been the federal government's role. Yet this is now becoming, in effect, a regulatory expectation. The industry is subject to mandatory and enforceable CIP standards that address both cyber and physical security. However, as cyber threats continue to evolve, the regulatory process by nature cannot keep pace. To address this challenge, the industry works closely with its government partners through the ESCC to quickly identify and mitigate new cybersecurity and other risks to the electricity subsector.

2. **Is there a uniform definition used in the energy and electricity sector – or at the federal level – of what cyber "secure" or "resilient" means?**

   Currently there is no universal or common agreement on the precise meaning of cyber "secure" or "resilient". The electric industry recognizes that it may not be able to prevent every outage, and is working to continually enhance its ability to rapidly respond and recover. The industry's philosophy is one of risk management, recognizing that every risk cannot always be predicted or eliminated. The industry works with government through mandatory reliability standards as well as the ESCC and other partnerships to identify and mitigate the key risks to the electricity sector. The reliability standards include ten cybersecurity standards and one physical security standard. The industry is working with

NERC to develop an eleventh cybersecurity standard focusing on minimizing supply chain cybersecurity risk.

3. **How costly is it to fund research RD&D for cyber from a utilities perspective? When updating your networks and physical infrastructure, are you able to put in new, more cyber secure equipment in select areas or does it need to be done across the board? Do you feel cyber security and resilient investments are adequately reflected in rate-making cases?**

   Cyber security research and development can be very costly. Many utilities participate in collaborative R&D initiatives in conjunction with EPRI, which is performing research in this space and is an important partner in developing risk mitigation strategies. DOE, especially through the National Labs, can also be a valuable partner, as can other federal agencies, such as DHS or DOD.

4. **Are customers appropriately knowledgeable on cybersecurity? How do we address that shortcoming?**

   It is our sense is that the general population faces significant challenges in maintaining awareness of current and emerging cyber security risk. The cyber threat is constantly evolving, and consequently customers and the general public are unlikely to be appropriately knowledgeable on cybersecurity. Constant communication and continual education on good cyber hygiene practices can help customers—as well as utilities through their own employees—significantly raise their defenses against cyber threats. Practices such as using strong passwords and passphrases, applying software patches, changing default administrative passwords, identifying and reporting phishing attempts, and knowing what devices are active on the network can considerably reduce customers' risk profiles, making them less of a target for cyber-crime and cyber attacks.