GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

February 23, 2017

Mr. Scott L. Aaronson
Executive Director
Edison Electric Institute
701 Pennsylvania Avenue, N.W.
Washington, DC 20004

Dear Mr. Aaronson:

Thank you for appearing before the Subcommittee on Energy on Wednesday, February 1, 2017, to testify at the hearing entitled "The Electricity Sector's Efforts to Respond to Cybersecurity Threats."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on March 9, 2017. Your responses should be mailed to Will Batson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Will.Batson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Fred Upton
Chairman
Subcommittee on Energy

cc: The Honorable Bobby Rush, Ranking Member, Subcommittee on Energy

Attachment

Additional Questions for the Record

The Honorable Fred Upton

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

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

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

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

      i. What is the state of research on this front?

      ii. What are the barriers to deployment?

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.

   A. 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?

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

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

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

   A. 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.

   B. 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?

The Honorable Morgan Griffith

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

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

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

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

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?

2. I'm also interested in how effective the current version of CIP standards are in mitigating the risks to utilities posed by cyberattackers. 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?

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 secure their cyberinfrastructure?

According to the Institute of Electrical and Electronics Engineers (IEEE or *I triple E*), 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?

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

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

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?

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?

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?

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

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