GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

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

February 23, 2017

Dr. Chris Beck
Chief Scientist and Vice President
for Policy
The Electric Infrastructure Security Council
840 First Street, N.E.
Washington, DC 20002

Dear Dr. Beck:

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

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

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

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

Sincerely,

Fred Upton
Chairman
Subcommittee on Energy

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

Attachment

Additional Questions for the Record

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. Beck, your organization focuses on Black Sky hazards. From the perspective of a cyberattack, such an event should be viewed as the worst case scenario: large in scope and duration, likely combining physical and cyberattacks to the grid, and potentially spanning across multiple critical infrastructure sectors.

1. Are the current norms and practices for electricity sector workforce training and development sufficient to prepare workers to respond quickly and effectively to the threat of an imminent or ongoing Black Sky attack?

2. What more could be done to improve electricity sector workforce training and development to better prepare workers for such event? In particular, can you speak to any efforts that would better promote intra-sector mutual assistance and cooperation across critical infrastructure sectors, both of which you promoted in your testimony?

It is certainly concerning that there are apparently not enough qualified applicants to fill the need for cybersecurity jobs in our country. I think this is a critical aspect of the issue that our Committee should evaluate as we continue our oversight of the security of our electric grid

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?

5. Electricity is one of our most critical infrastructures. And our ability to respond to natural disasters or attacks requires access to electricity. Your testimony touched on power grid restoration and the need for cross-sector planning. First, do you believe there's adequate cross-sector planning as of now? Does the electricity sector have sufficient capability to communicate and respond to emergency situations?

6. There have been an increasing number of new technologies placed onto the grid in the past decade. Protection throughout the supply chain is an area that deserves our attention, and that standards and best practices should be implemented but not overly prescriptive.

7. Are there concerns about potential cyber threats from systems that are already in place but we haven't seen an incident from yet?