GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

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

February 23, 2017

Mr. Gerry W. Cauley
President and CEO
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005

Dear Mr. Cauley:

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

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

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

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

Sincerely,

Fred Upton
Chairman
Subcommittee on Energy

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

Attachment

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?

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

One emerging challenge in grid security relates to the thousands of businesses, vendors and suppliers that make up the electric sector supply chain. There are several high profile examples from the retail sector where breaches to such third-party entities ultimately have caused direct harm to the first-party organization.

Mr. Cauley, in your testimony, you mention that modification of the Critical Infrastructure Protection (CIP) Standards are under development to address such challenges in supply chain management.

1. Can you provide an update on the development timeline for any new requirements to the CIP Standards to address supply chain cybersecurity issues? In particular, when will such modification be finalized?

2. In light of these pending new requirements, what options or best practices are available now for utilities to ensure the cybersecurity of their supply chain partners?

A related challenge is the security risks posed to utilities that using Internet of Things (IoT) and cloud-based technologies to move the vision of a "Smart Grid" closer to reality. IoT technologies, which connect devices to networks for the collection and exchange of data, hold great potential to revolutionize our way of life. Unfortunately, they also allow for many new entry points to the electric grid for hackers.

3. Do current cybersecurity standards address vulnerabilities to utilities posed by IoT devices?

4. Will the update to the CIP standards to address supply chain cybersecurity also be sufficient for addressing risks posed by IoT devices? And if not, how must utilities adapt their cybersecurity measures to best protect themselves from the risks posted by IoT technologies?

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. Given the dynamic changes happening at the distribution level, are there adequate measures in place across the country to ensure the same type of oversight and protection that occurs on the bulk power system? Are there ways for the distribution system to become a threat to the bulk power system reliability?

6. Most outages occur on the distribution side and not the bulk power system. It's my understanding that NERC uses a number of indicators, like the System Average Interruption Duration Index, which is calculated on a monthly or yearly basis.

7. You mentioned that the GridEx III participants were encouraged to share lessons learned. Out of the thousands who were involved, how many provided the feedback you asked for?

8. Your testimony stated that there has been no loss of load due to a cyber-attack. Would you like to expand on that?