NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

March 10, 2017

The Honorable Fred Upton
Chairman
Subcommittee on Energy
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Chairman Upton:

On behalf of the North American Electric Reliability Corporation, thank you for inviting me to testify before the Subcommittee on Energy on Wednesday, February 1, 2017, at the hearing entitled, “The Electricity Sector’s Efforts to Respond to Cybersecurity Threats.” Attached are my responses to questions for the record.

Again, we greatly appreciate the opportunity to support the important work of the subcommittee.

Sincerely,

[redacted]

Gerry W. Cauley
President and Chief Executive Officer

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

Attachment

Responses from Gerry W. Cauley
President and CEO
North American Electric Reliability Corporation

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.

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

NERC and industry have several ways in which we are developing and supporting policies related to strengthening system components. NERC's robust Critical Infrastructure Protection (CIP) standards are designed to protect critical electric infrastructure, thereby resulting in procurement of advanced technologies necessary to comply with CIP requirements. In addition, FERC ordered NERC to develop a new CIP standard to address supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.

NERC also has a standing technical committee, the Critical Infrastructure Protection Committee (CIPC), that helps NERC advance the physical and cyber security of the critical electricity infrastructure of North America. The committee consists of both NERC-appointed regional representatives and technical subject matter experts. CIPC coordinates NERC's security initiatives and serves as an expert advisory panel to the NERC Board of Trustees, standing committees in the areas of physical security and cybersecurity, and the Electricity Information Sharing and Analysis Center (E-ISAC).

NERC's E-ISAC works closely with the Electricity Subsector Coordinating Council (ESCC), supporting policy development efforts through the ESCC's various working groups. The ESCC's Research and Development Working Group collaborates closely with the Department of Energy (DOE) on initiatives to address strengthening system components.

NERC recently shared information with industry concerning the Internet of Things (IoT) vulnerability. On October 11, 2016, NERC issued a non-public Level 2 Alert, "Internet of Things (IoT) Used for High Bandwidth Distributed Denial of Service (DDoS) Attacks." Also, the E-ISAC published an Internet of Things DDos White Paper on October 24, 2016, providing recommendations for defensive capabilities in the Electricity Subsector, with suggestions for improving the overall posture of network security and cybersecurity.[1] NERC also issued a non-public Level 2 Alert with recommendations on February 9, 2016, regarding the events that occurred in Ukraine, followed by the posting of the joint team analysis on March 21, 2016, to provide a lessons learned resource from event. These efforts help to inform industry about the vulnerabilities in system components that were vectors in those attacks.

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

The U.S. Department of Energy (DOE), the National Institute of Standards and Technology, and trade organizations from the electric power and manufacturing industries have developed best practices and guidelines, which cover various procurement and supply chain cyber security risk management practices.

DOE's Office of Electricity Delivery and Energy Reliability has developed the Cybersecurity Capability Maturity Model (C2M2). C2M2 is a voluntary evaluation process utilizing industry-accepted cybersecurity practices that can be used to measure the maturity of an organization's cybersecurity capabilities. The C2M2 is designed to measure both the sophistication and sustainment of a cyber security program. The model was identified, organized, and documented by energy sector subject matter experts from both public and private organizations.[2] NERC provided DOE with technical expertise and industry outreach support during development of the C2M2 model.

In addition, DOE and NERC regularly work together to provide threat and vulnerability briefs to stakeholders. Several DOE presentations on supply chain issues, as well as research and development (R&D) programs, have been briefed to industry stakeholders at NERC conferences, including National Laboratory projects and the Cybersecurity for Energy Delivery Systems (CEDS) R&D program. NERC and the E-ISAC collaborate often with DOE and their national labs systems on a regular basis. For example, DOE provided input helping support the E-ISAC in development of the GridEx IV scenario. The E-ISAC and DOE also coordinate during regular synch meetings to discuss current threats and vulnerabilities.

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?

NERC encourages industry participation in security-related pilot programs and broader efforts through DOE and other sources to increase protection from cyber attacks. Some programs include the California Energy Systems for the 21st Century (CES-21) program, the Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program, and others. NERC facilitates sharing

[1] *The white paper is posted to the E-ISAC website at* https://www.eisac.com/.

[2] *See DOE fact sheet at* https://energy.gov/sites/prod/files/2014/02/f7/C2M2-FAQs.pdf.

technology briefs about these programs with stakeholders, and is working with the RADICS team to deploy tools to industry in conjunction with GridEx IV and V.

Industry participants have also worked with the Department of Energy to draft the DOE guidelines on *Cybersecurity Procurement Language for Energy Delivery Systems* (https://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014). Further, the Edison Electric Institute developed a set of key principles and recommendations for entities to consider for managing supply chain cybersecurity risks (http://www.eei.org/issuesandpolicy/testimony-filings-briefs/Documents/150917FinalEEIPrinciplesandResourcesforManagingSupplyChainCybersecurityRisk.pdf).

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

NERC would defer to the Department of Energy as well as the Electric Power Research Institute (EPRI) on this question.

ii. What are the barriers to deployment?

From NERC's standpoint, one challenge for deployment of new technology is that it must be proven to be reliable over time in a variety of conditions. In addition, the full consequences of the use of new technology must be understood. Because the electricity system is an interconnected network, any changes in one component may have consequences for the use or operation of other components.

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?

The E-ISAC is a leading, trusted source for the analysis and sharing of electricity industry security information. The E-ISAC reduces cyber and physical security risk to industry across North America by providing unique insights, leadership, and coordination. One of the E-ISAC's central roles is to connect industry and government. To accomplish this, the E-ISAC works closely and regularly with the National Cybersecurity and Communications Integration Center—the central means for the federal government to aggregate and share information on cyber threats. In addition, NERC works closely with the ESCC to further the public private partnership dialogue addressing security and resilience matters. Maintaining this partnership is key to ensuring private and public sector communications regarding threats and intelligence sharing.

To achieve better coordination, the federal government can enhance the clearance process to ensure appropriate industry individuals are cleared at the appropriate levels to receive classified information and provide subject matter expertise. In addition, the government can work to downgrade classified information when feasible for industry that is timely and actionable. Finally, the government can assist industry by ensuring access to local classified briefing spaces so that industry subject matter experts can receive information and provide input and advice from an asset owner and operator perspective.

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?

CRISP is an important partnership between DOE, NERC and the industry, providing critical security information to entities serving 75% of electricity customers in the United States. NERC and the E-ISAC are working with DOE on other initiatives that may enhance the CRISP programs, including extending CRISP into the operational technology environment. DOE has also initiated a grant program with electricity industry trade associations focused on improving the cyber and physical security culture for members of the National Rural Electric Cooperative Association and the

American Public Power Association. The grant will develop security tools, provide educational resources, update security guidelines, and offer training.

In addition, the Department of Defense is partnering with NERC, the E-ISAC, and industry asset owners and operators to deploy and evaluate tools and technologies for grid security through the RADICS program.

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?

FERC Order No. 829, directs NERC to develop by September 27, 2017 a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. The new or modified Reliability Standard is intended to mitigate the risk of a cybersecurity incident affecting the reliable operation of the bulk power system. The order stated that the new or modified Reliability Standard should address the following security objectives: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. In FERC Docket No. RM15-14-002, NERC filed its complete project plan outlining the timeline for completing this standard.[3]

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?

Best practices and guidelines have been developed by the U.S. Department of Energy, the National Institute of Standards and Technology, and trade organizations from the electric power and manufacturing industries. These cover various procurement and supply chain cyber security risk management practices.

Some examples are:

Cybersecurity Procurement Language for Energy Delivery Systems
http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

Cybersecurity Procurement Language for Control Systems Version 1.8
http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SCADA_Procurement_Language.pdf

National Electrical Manufacturers Association (NEMA) Supply Chain Best Practices Guideline

[3] *See* http://www.nerc.com/pa/Stand/Pages/Project201603CyberSecuritySupplyChainManagement.aspx.

Document CPSP 1-2015
http://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx#download

Supply Chain Risk Management Practices for Federal Information Systems and Organizations
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

"Principles and Resources for Managing Supply Chain Cybersecurity Risk"
http://www.eei.org/issuesandpolicy/testimony-filings-briefs/Documents/150917FinalEEIPrinciplesandResourcesforManagingSupplyChainCybersecurityRisk.pdf

In addition, NERC continues to monitor and communicate the security risks posed to the Bulk Power System by the increased use of Internet of Things (IoT). On October 11th, 2016, NERC issued a non-public Level 2 Alert, "Internet of Things (IoT) Used for High Bandwidth Distributed Denial of Service (DDoS) Attacks." Also, the Electricity Information Sharing and Analysis Center (E-ISAC) published an Internet of Things DDos White Paper in October 24, 2016 providing recommendations for defensive capabilities in the Electricity Subsector, with suggestions for improving the overall posture of network security and cybersecurity.[4]

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

The CIP standards afford protections and safeguards to the "Industrial" Internet of Things where over the past decade we have a observed a substantial increase in the number of intelligent devices deployed throughout the bulk power system that if compromised could have some real impacts to reliability. NERC's CIP standards have evolved to better address new and dynamic threats. Reliability Standards are a necessary foundation to address the vulnerabilities to utilities posed by IoT devices, but they are not sufficient alone to protect against these evolving threats. Monitoring and communication with timely information exchange is essential.

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?

FERC directed NERC to develop a standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. This standard is currently under development. Once approved by FERC, this standard would focus on the security of the products acquired by entities subject to the standard. Currently enforceable CIP standards requirements, which include methods to identify industry intelligent systems used to operate the grid, network security, malware protection,

[4] *The white paper is posted to the E-ISAC website at* https://www.eisac.com/.

incident response as well as other security controls, are in place to further protect assets being used to operate the grid.

In response to risks posed by IoT devices, and as noted above, NERC issued a non-public Level 2 Alert regarding the IoT vulnerability. The E-ISAC also published an Internet of Things DDoS White Paper to provide recommendations for defensive capabilities in the electricity sector and suggestions to improve the overall posture of network security and cyber security.

5. 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?

In 2016, 128 registered entities reported noncompliance with CIP standards. This figure accounts for 10% of NERC registered entities subject to CIP standards. A majority of these reports are still under review.

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?

NERC receives no funding from federal agencies. As noted in my testimony, NERC derives considerable technical expertise from federal agencies through partnerships and collaboration with DOE, DHS, and NIST. In addition, FERC provides technical expertise for a wide range of NERC activities through formal and informal means, including the reliability standard review process and many other programs. Continued support for these partnerships remains important.

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?

In the Energy Policy Act of 2005, Congress expressly included "cybersecurity protection" when it defined the scope of "reliability standards" in Federal Power Act (FPA) Section 215(a)(3). NERC agrees that physical and cybersecurity threats are a growing concern. NERC and our government and industry stakeholders have been and remain focused on them.

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?

NERC defines security and resiliency through the use of our standards and information sharing efforts. As we have discussed, this is part of a collective approach to risk, with standards providing a strong foundation for a reliable and secure BPS.

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?

NERC defers to individual utilities to provide perspective on research funding and recovery of cyber and resilient investments in rate cases.

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

NERC's registry contains nearly 1,500 users, owners and operators of the Bulk Power System. Through the E-ISAC, NERC reaches even more electric system entities and provides them with information. This is an ongoing challenge, but working together with our federal government partners, with state regulators and with utilities, Regional Transmission Organizations, customers and experts, we are trying to increase the level of awareness of cybersecurity threats and what can be done to address them.

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?

NERC's jurisdiction includes users, owners, and operators of the bulk power system (BPS). "Facilities used in the local distribution of electric energy" are excluded from the definition of the "bulk-power system" under FPA Section 215, and are regulated by the states. However, NERC's jurisdiction does extend to certain distribution providers connected to the BPS that impact over 300MW of automatic load shedding. In other words, certain distribution providers that could impact reliable operation of the BPS are subject to CIP standards.

E-ISAC's information sharing portal has reach to distribution providers. While NERC's jurisdiction is focused on the BPS, all distribution providers are eligible to become members of the E-ISAC portal, even distribution providers that are not connected to the BPS. Therefore, distribution providers that are members of the E-ISAC portal benefit from cyber and physical security information from the E-ISAC.

NERC recently issued the Distributed Energy Resources Connection and Modeling and Reliability Considerations assessment. The report discusses potential reliability risks and mitigation approaches for increased levels of distributed energy resources on the BPS. DER will increasingly have state-of-the-art capabilities for active power control and reliability services. However, there are differences in how DER are deployed within the grid and the characteristics of the services and responses that they provide, so these differences must be understood and modeled appropriately. As a result, this report explains how practices for modeling and operating the BPS may be enhanced to reflect future system characteristics. It is paramount that NERC and the industry understand DER functionality and develop a set of guidelines to assist in modeling and assessments such that owners/operators of the BPS can evaluate and model DER in the electric system. The report is meant to help entities, regulators, and policy makers better understand the differences between DER and conventional generation and how DER affect the BPS.

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.

SAIDI (System Average Interruption Duration Index) and SAIFI (System Average Interruption Frequency Index) are metrics that are widely used by industry to assess reliability on their distribution systems. As NERC's focus is on the BPS, NERC utilizes the SRI, or Severity Risk Index. The SRI is a measure of stress to the BPS in any day resulting from generation loss, transmission loss, or load loss components. The SRI is a key metric in NERC's annual State of reliability report which assesses the reliability performance of the BPS.

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?

Thousands of individuals participated in GridEx III. In collecting responses from industry, the E-ISAC focused on obtaining feedback from organizations and lessons learned that had not been identified in previous exercises. NERC issues a public report after each GridEx.[5] For GridEx III, NERC received 25 lessons learned reports, representing about 24 percent of active participating utility organizations. These lessons learned represent opportunities for industry to identify possible initiatives to enhance response to cyber and physical attack or improve future exercises of this nature.

[5] *See GridEx III report at* http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx.

Voluntary submissions from organizations have continued to increase with each successive GridEx exercise. We anticipate this trend will continue.

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

As you point out, there has not been any loss of load in North America that can be attributed to a cyber attack. This recognizes the commitment of industry and the effectiveness of complementary strategies discussed in my testimony. However, we cannot be complacent. We must remain vigilant in assuring the reliability and security of the bulk power system.