Testimony of James B. Robb, President and Chief Executive Officer
North American Electric Reliability Corporation

Before the Senate Committee on Energy and Natural Resources
"Status and Outlook for Cybersecurity Efforts in the Energy Industry"

February 14, 2019

Introduction

Good morning Chairman Murkowski, Ranking Member Manchin, members of the committee and fellow panelists. My name is Jim Robb and I am the President and CEO of the North American Electric Reliability Corporation (NERC). NERC's mission, as the Electric Reliability Organization (ERO) certified by the Federal Energy Regulatory Commission (FERC), is to assure the reliability and security of the bulk power system (BPS) in North America. The threat of cyber attacks by nation states, terrorist groups, and criminals is at an all-time high. Now more than ever, grid security is inextricably linked to reliability. The North American BPS is among the nation's most critical infrastructures. Virtually every critical sector depends upon electricity. The BPS is also one of the largest, most complex systems ever created. It is robust and highly reliable. Nevertheless, conventional and non-conventional factors do present risks to the BPS.

I have been at NERC for nine months and prior to NERC served as the CEO of WECC, the Western Electricity Coordinating Council, one of seven regions in the reliability enterprise. I have more than 30 years of experience working with the electricity industry and am pleased to speak with you today about NERC's responsibilities for grid security.

Summary

The security landscape is dynamic, requiring constant vigilance and agility. NERC assures grid security through a comprehensive series of complementary strategies involving mandatory standards, information sharing, and partnerships. NERC's mandatory critical infrastructure protection standards (CIP standards) are a foundation for security practices. They provide universal, baseline protections. Due to the ever-evolving nature of cyber threats, security cannot be achieved through standards alone. Vigilance also requires the agility to respond to new and rapidly changing events. Accordingly, NERC's Electricity Information Sharing and Analysis Center (E-ISAC) serves as the information sharing conduit both within the North American electricity industry and between the electricity industry and government for cyber and physical security threats. The E-ISAC facilitates communication of important or actionable information, and strives to determine and maintain "ground truth" during rapidly evolving security events. The E-ISAC also plays a key role in cross-sector coordination, focusing on sectors with which electricity has interdependencies, such as natural gas, water, and other critical infrastructure. Mandatory standards, coupled with effective mechanisms to share information, provide robust and flexible tools to protect the BPS. NERC works closely with the Department of Energy (DOE), Department of Homeland Security (DHS), FERC, and the Electricity Subsector Coordinating Council (ESCC) to further the public-private partnership so important to addressing security. NERC's biennial GridEx exercise is the largest of its kind in the sector and helps industry and government exercise their emergency response plans, and drive new and innovative approaches to reduce security risk to the electric grid.

About NERC

NERC is a private non-profit corporation that was founded in 1968 to develop voluntary operating and planning standards for the users, owners and operators of the North American BPS. Pursuant to Section 215 of the Federal Power Act (FPA) (16 U.S.C. §824o) and the criteria included in Order No. 672 for designating an Electric Reliability Organization (ERO), FERC certified NERC as the ERO for the United States on July 20, 2006. On March 16, 2007, FERC issued Order No. 693 which approved the initial set of reliability standards. These reliability standards became mandatory in the United States on June 18, 2007.

NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC performs a critical role in real-time situational awareness and information sharing to protect the electricity industry's critical infrastructure against threats to the BPS. NERC's area of responsibility spans the continental United States, Canada, and Mexico. Our jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

Critical Infrastructure Protection Standards

With oversight from FERC, NERC is responsible for developing and enforcing mandatory reliability standards for the BPS. The CIP standards provide a common, universal foundation for security. They are robust and comprehensive, covering a wide range of priorities and threat vectors.

More than a decade ago, Congress had the foresight to anticipate the emerging risk posed by cyber security threats to the BPS by defining reliability standards to include "cybersecurity protection." NERC's CIP standards are developed by registered entities through an open, transparent stakeholder process, subject to approval by NERC's Board of Trustees and FERC. In addition, FERC can order NERC to develop a standard and has done so on topics such as geomagnetic disturbances, physical security, and supply chain cyber security risk management.

The CIP standards group includes the following 12 topics addressing cyber and physical security:[1]

CIP-002 – Cyber System Identification and Categorization requires entities to identify their cyber systems that perform reliability functions and must be protected under the CIP standards. Using bright-line criteria, this standard also requires entities to categorize these systems as "high," "medium," or "low" impact based on the risk to the BPS if the system were compromised. This categorization forms the basis for determining the level of controls applied to those systems under the applicable CIP standards.

CIP-003 – Security Management Controls and Requirements for Lower Risk Cyber Systems requires entities to adopt and maintain cyber security policies to establish responsibility and accountability for protecting critical cyber systems. This standard also identifies the security controls for those systems identified as low impact focusing on: cyber security awareness;

[1] To view NERC CIP standards, see http://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=United%20States.

physical access controls; electronic access controls; cyber security incident response; and protections for transient electronic devices (e.g., thumb drives, laptop computers).

CIP-004 – Personnel and Training establishes rules for authorizing personnel, including contractors and service vendors, for electronic or unescorted physical access to high- and medium-impact cyber systems. It also establishes rules for ensuring these personnel have the appropriate level of training and security awareness.

CIP-005 – Electronic Security Perimeters establishes rules for managing electronic access to high and medium impact cyber systems through use of electronic security perimeters that delineate a "trust zone." This standard also establishes rules for remote access to these cyber systems.

CIP-006 – Physical Security of Cyber Systems establishes rules for managing physical access to high- and medium-impact cyber systems.

CIP-007 – Systems Security Management addresses system security by specifying technical, operational, and procedural requirements in support of protecting high- and medium-impact cyber systems.

CIP-008 – Incident Reporting and Response Planning specifies incident reporting and response requirements.

CIP-009 – Recovery Plans specifies recovery plan requirements to help ensure that reliability functions are recovered following a cyber security incident.

CIP-010 – Change Management and Vulnerability Assessments specifies system configuration management and vulnerability assessment requirements to help prevent and detect unauthorized changes to high- and medium-impact cyber systems.

CIP-011 – Information Protection establishes rules to prevent unauthorized access to cyber system information by specifying information protection requirements.

CIP-013 – Cyber Security Supply Chain Management will require entities to develop and implement a plan to address supply chain cyber security risks during the planning and procurement of industrial control system hardware, software, and services. This standard was approved by FERC on October 18, 2018, and will become effective on July 1, 2020.
This standard was approved by FERC on October 18, 2018, and will become effective on July 1, 2020.

CIP-014 – Physical Security of Critical Transmission Substations and Associated Control Centers that pose the greatest risk to reliability if they are damaged or rendered inoperable due to physical attack. The standard requires entities to determine what facilities are critical, assess the physical security threats to and vulnerability of those critical facilities, and implement a plan to mitigate those threats and vulnerabilities.

As experience and technology continue to grow, NERC, with FERC oversight, continues to refine and improve the CIP standards to help ensure their effectiveness and timeliness. For example, pending before FERC is a new CIP standard, CIP-012, that would require enhanced protections of sensitive data transmitted between critical control centers. Additionally, at its February 2019 meeting, the NERC Board of Trustees adopted revisions to CIP-008 to enhance reporting of cybersecurity incidents. This revised standard will be filed for FERC approval in the near future. NERC is also currently working with industry experts to consider modifications to the CIP standards to better account for technological innovation.

Electricity Information Sharing and Analysis Center

NERC's CIP standards provide a universal foundation for security practices. Yet security cannot be achieved through these standards alone. Because of the emerging and dynamic nature of malicious cyber threats, reliability assurance also requires constant situational awareness, real time communication, and prompt emergency response capabilities. The E-ISAC provides these services and supports these industry capabilities.

The mission of the E-ISAC is to reduce cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration. It accomplishes this mission by sharing trusted information and analysis in a timely, credible, actionable manner with asset owners and operators across the continent.

Operated by NERC, and working in collaboration with the DOE and the ESCC, the E-ISAC is the central information sharing hub for the electricity sector. The E-ISAC uses a secure portal as the primary means for communicating with its more than 1,025 electricity industry member organizations, and the number continues to grow. The portal was revamped in 2017 and is constantly undergoing further upgrades to enhance the user experience. The new portal functions, plus greater outreach with key industry stakeholder groups through our Industry Engagement Program (IEP), has improved bi-directional information sharing and allows members greater access to more information.

E-ISAC services enable industry to defend against and respond to cyber and physical security threats, vulnerabilities, and incidents through the exchange of timely, actionable information. In addition to coordination with DOE and FERC's Office of Infrastructure Security, the E-ISAC promotes cross-sector coordination through work with the DHS and other agencies and ISACs. In particular, to further enhance cross-sector collaboration in light of electric and natural gas interdependencies, the E-ISAC continues to expand its partnership with the Downstream Natural Gas ISAC (DNG-ISAC). In the past year, the E-ISAC added additional partnerships with other interdependent sectors, including the Water-ISAC and the Multi-State ISAC with the goal providing electricity sector context to water and waste-water operators, as well as state and local governments. Security is a global priority, and because NERC is an international organization, the E-ISAC works with Natural Resources Canada, Public Safety Canada, and the recently established Canadian Centre for Cyber Security to provide cross-border outreach and collaboration. In October 2018, NERC announced a trilateral memorandum of understanding among the E-ISAC, the Japan Electricity ISAC and the European Energy ISAC with the intention of expanding sources of information and opportunities for analysis with partners who face similar adversarial threats. As the E-ISAC moves to 24/7 watch operations, these international partnerships will provide valuable context and awareness of emerging threats for overnight analysts to share with North American grid operators

Cybersecurity Risk Information Sharing Program (CRISP)

Managed by the E-ISAC and in partnership with DOE, CRISP uses innovative technology and leverages DOE and its National Laboratory System's analytical capability. CRISP provides timely bi-directional sharing of unclassified and classified threat information and develops situational awareness tools to enhance the electricity sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure. CRISP companies cover more than 75 percent of U.S. customers. CRISP information is shared in a secure fashion through the E-ISAC portal, and allows non-CRISP member companies to benefit from the shared indicators and threat actor activity captured by the program. CRISP information also supports the development of situational awareness to enhance the industry's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources. In addition to CRISP, the E-ISAC is pursuing cyber automated information sharing systems as well as a malware analysis repository and threat information exchange to provide for more advanced information sharing capabilities.

NERC Alerts, Critical Broadcasts, and Briefings

In addition to the secure portal, the E-ISAC shares information through a number of forums to increase awareness of threats, and to recommend mitigation. When there is a significant security concern, NERC and the E-ISAC communicate with the electricity industry via two distinct platforms.

NERC alerts provide concise, actionable security information to the electricity industry. Security alerts communicate unclassified sensitive information and mitigation measures. Alerts are divided into three levels:

- Level One – Industry Advisory: Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.
- Level Two – Recommendation to Industry: Recommends specific action be taken by registered entities. Requires a response from recipients as defined in the alert.
- Level Three – Essential Action: Identifies actions deemed to be "essential" to BPS reliability and requires NERC Board of Trustees approval prior to issuance. Like recommendations, essential actions require recipients to respond as defined in the alert.

NERC determines the appropriate alert notification based on risk to the BPS. Generally, NERC distributes alerts broadly to users, owners, and operators of the North American BPS using its compliance registry. Entities registered with NERC are required to provide and maintain updated compliance and cyber security contacts. NERC also distributes the alerts beyond BPS users, owners, and operators to include other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g., balancing authorities, transmission operators, generation owners, etc.).
Alerts are developed with the strong partnership of federal technical organizations, including FERC, DOE National Laboratories, DHS, and BPS subject matter experts. Since 2009, NERC has

issued 46 security-related alerts, 41 of which were cyber-related (41 Industry Advisories and 5 Recommendations to Industry). Those alerts covered items such as sabotage events, pandemic, Aurora, Night Dragon, and heightened awareness and reporting guidance of suspicious activity. In 2016, NERC issued two Level Two alerts – the first related to the 2015 cyber-attack in Ukraine and another concerning distributed denial of service attacks leveraging compromised Internet of Things[2] devices. Responses to alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders.

In addition to NERC alerts, the E-ISAC uses the Critical Broadcast Program (CBP). This program launched in 2018 to rapidly share information with members. The CBP capability is designed to rapidly disseminate critical security information to the electricity industry. The CBP leverages E-ISAC staff and stakeholder expertise to obtain and share the best available information and potential mitigation strategies to address developing security threats and events in a timely manner. The information is shared through the E-ISAC portal and other means, as necessary. The E-ISAC used this capability four times in 2018: on February 7, where 1,208 individuals joined the call; February with 2,960 individuals; November 29, with 524 participants; and December 20, where more than 1,284 individuals from the electricity and oil and natural gas subsectors joined the call.

The E-ISAC also hosts regular monthly threat briefings, unclassified threat workshops, classified forums for its members, and allows asset owners and operators to interact with our analysts and each other to share trend analysis and context on common threats to the electricity sector. In addition to the regularly hosted events, the E-ISAC conducted seven sessions of IEP in 2018, a three-day session where industry members visit the E-ISAC to see firsthand how the E-ISAC operates on a daily basis. These activities allow members to discuss emerging threats, learn from security experts, and provide feedback directly to the E-ISAC—which help improve E-ISAC's products and services.

GridEx

Consistent with our mission to promote a strong learning environment, NERC hosts an every other year grid security exercise – GridEx – which simulates widespread, coordinated cyber and physical attacks on critical electric infrastructure designed to overwhelm even the most prepared organizations. GridEx is the largest geographically distributed grid security exercise for the electricity sector. It consists of a two-day distributed play exercise and a separate executive tabletop session. GridEx allows participants to:

- Exercise crisis response and recovery;
- Improve communication;
- Identify lessons learned; and
- Engage senior leadership.

[2] The Internet of Things (IoT) refers to devices and sensors connected to the Internet such as security cameras, alarm systems, printers, or light switches. IoT devices typically use default passwords and are highly vulnerable to subversion by threat actors.

In 2017, 6,500 individuals and 450 organizations participated in GridEx IV, including industry, law enforcement, and government agencies. The executive tabletop included 42 participants from a cross-section of industry executives and senior officials from federal and state governments. Participating organizations are encouraged to identify their own lessons learned and share them with NERC. NERC uses this input to develop observations and propose recommendations to help the electricity industry enhance the security and reliability of North America's BPS. We are deep into planning for GridEx V which will be conducted on November 13-14, 2019.

GridSecCon

Consistent with promoting a learning environment and information exchange, NERC hosts the annual Grid Security Conference (GridSecCon). This widely attended conference brings together cyber and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity industry. While the specific agenda varies from year to year, general objectives include:

- Promoting reliability of the BPS through training and industry education;
- Delivering cutting-edge discussions on security threats, vulnerabilities, and lessons learned from senior industry and government leaders; and
- Informing industry with discussions on security best practices, reliability concerns, risk mitigation, and cyber and physical security threat awareness.

Cyber Threats and Trends

These engagements and analytical capabilities have increased the E-ISAC's insight into threats to the grid. This greater insight has translated into more security products for industry, as well as more member-originated information submitted to the E-ISAC and more sharing. In 2018, more than 300 cyber bulletins and more than 200 physical bulletins were posted to the portal. The E-ISAC also posts bulletins based on information obtained from government partners and trusted open source partners, and we thank our government partners at DOE, DHS, and FBI for continuing to produce these valuable products.

Looking at the trend analysis of those bulletins, the major cyber and physical security trends of 2018 included: cryptojacking, phishing, malware, gunfire at electric infrastructure, and theft. From a cyber perspective, the threat constantly changes, and members must be vigilant, staying informed about adversaries' latest tactics, techniques, and procedures. While many physical security threats remain similar from year-to-year, the threat from activist groups continue to evolve as they become more capable.

In 2018, many familiar malware families such as Shamoon and GreyEnergy—the successor to BlackEnergy—saw new variants, while other frameworks like VPNFilter first appeared. In the case of VPNFilter, the E-ISAC leveraged its partnership with an industrial control system vendor to quickly dispel concerns regarding the Modbus module's capabilities. The threat, however, is clear: advanced attackers continue to develop highly modular tools with the ability to greatly impact a targeted system.

Cyber Security Threat Outlook

As the E-ISAC looks to the future, we anticipate certain trends:

Credential harvesting: Tactics to acquire legitimate user credentials to gain initial access to targeted networks and establish persistence mechanisms will continue to be popular because it helps evade detection. Sophisticated spear phishing activity to harvest credentials is the most common technique observed by members.

Exploitation of the trust relationship between targeted organizations and their business partners: Recent incidents have demonstrated that nation-state adversaries are targeting the electric sector and other industries by compromising the networks of third parties with which the intended targets have established business relationships. This tactic is a type of supply chain attack, and increases the success rate of tactics used to initially compromise the intended target.

Network device targeting: From the high profile reports on VPNFilter to the state-sponsored actors targeting network devices discussed in United States, switches and routes located on the edge of networks are a prime target for threat actors capable of intercepting and processing a large amount of information. Because these devices are placed at the boundary between internal networks and the internet, and exist to allow controlled access to the internal network, they will most likely continue to be a target of reconnaissance.

Use of native tools: Adversaries will likely continue to use tools and capabilities already present on a compromised network – such as PowerShell or Windows Management Infrastructure (WMI) – to conduct reconnaissance, lateral movement, and privilege escalation. The presence or use of these tools on a targeted network is unlikely to raise alarm, so their inappropriate use helps evade detection.

Conclusion

Reliability is NERC's mission, and grid security is inextricably linked to reliability. To date, there has not been any loss of load in North America that can be attributed to a cyber attack. At the same time, the security landscape is dynamic, requiring constant vigilance and agility. NERC addresses cyber threats through a comprehensive range of complementary strategies. Our partnership with DOE is critical to the electricity subsector's priority for security. Mandatory CIP standards provide a universal foundation for security and is a shared priority with FERC and industry. Through the E-ISAC, NERC provides situational awareness, and sharing of timely, actionable intelligence with industry and government. Strong public private partnerships are key to successful information sharing within the electricity sector and across sectors. NERC remains keenly focused on our mission to assure reliability of the BPS.