Testimony of Gerry W. Cauley, President and Chief Executive Officer

North American Electric Reliability Corporation

Before the Subcommittee on Energy of the House Energy and Commerce Committee

"The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

February 1, 2017

Good morning Chairman Upton, Ranking Member Rush, members of the subcommittee and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). I am pleased to speak with you today about the responsibilities that Congress has vested in NERC to assure the reliability and security of the bulk power system (BPS) in North America. Given the topic of today's hearing, my testimony focuses on NERC's role in addressing cyber security threats.

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.

Summary

The security landscape is dynamic, requiring constant vigilance and agility. NERC addresses cyber risk through a variety of regulatory and non-regulatory means. Today's testimony will focus on those efforts currently underway by NERC to address cyber security and protect the grid. 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 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 maintain "ground truth" during rapidly evolving security events. Together, mandatory standards, coupled with effective mechanisms to share information, provide robust and agile tools to protect the BPS. NERC works closely with the Electricity Subsector Coordinating Council (ESCC) to further the public private partnership so important to addressing security.

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 the northern portion of Baja California, Mexico. Our jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

Critical Infrastructure Protection Standards

With oversight by FERC, NERC is responsible for developing and enforcing mandatory reliability and security standards for the BPS. More than a decade ago, Congress had the foresight to anticipate the emerging risk posed by cyber security threats to the BPS. The Energy Policy Act of 2005 expressly states that reliability standards extend to "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.

Currently, NERC is implementing the fifth version of the CIP standards which include the following 11 topics addressing cyber and physical security:[1]

Cyber System Categorization – Identifies and categorizes bulk electric cyber systems and their associated cyber assets (CIP-002-5.1a). This categorization is used as a basis for determining the level of controls applicable to those systems in the rest of the CIP cyber security standards.

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

Security Management Controls – Specifies consistent and sustainable security management controls (CIP-003-6). This standard also identifies the security controls for those systems identified as "low impact" under CIP-002-5.1.

Personnel and Training – Requires that personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. (CIP-004-6).

Electronic Security Perimeters – Requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter (CIP-005-5).

Physical Security of BES Cyber Systems – Requires a physical security plan in support of protecting BES cyber systems (CIP-006-6).

Security System Management – Specifies technical, operational, and procedural requirements in support of protecting BES Cyber Systems (CIP-007-6).

Incident Reporting and Response Planning – Specifies incident reporting and response requirements (CIP-008-5).

Recovery Plans for BES Cyber Systems – Specifies recovery plan requirements in support of the continued stability, operability, and reliability of the BES (CIP-009-6).

Configuration Change Management and Vulnerability Assessments – Prevents and detects unauthorized changes to BES cyber systems by specifying configuration change management and vulnerability assessment requirements (CIP-010-2).

Information Protection – Prevents unauthorized access to BES cyber system information by specifying information protection requirements in support of protecting BES cyber systems against compromise (CIP-011-2).

Physical Security – Requires identification and protection plans for certain "grid-critical" transmission stations and transmission substations, and their associated primary control centers (CIP-014-2).

In addition to these 11 currently enforceable standards, NERC is currently developing a new standard pursuant to FERC directive to address supply chain cyber security risk.

Cyber Security Supply Chain Management (Under Development) – Requires entities to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations (CIP-013-1).

Electricity Information Sharing and Analysis Center

NERC's CIP standards provide a foundation for security practices. They provide universal, baseline protections. But 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. NERC operates the E-ISAC which is a key component in providing these capabilities for the electric sector.

The E-ISAC, in collaboration with the Department of Energy (DOE) and the ESCC, serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

The E-ISAC:[2]

- Identifies, prioritizes, and coordinates the protection of critical power services, infrastructure service, and key resources;
- Facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and practices;
- Provides rapid response through the ability to effectively contact and coordinate with asset owners and operators, as required;
- Authors alerts to industry ranging from advisory notices to essential actions requiring recipients to respond as defined in the alert;
- Provides and shares analysis, which includes capturing and correlating trend data for historical analysis, and sharing that information within the sector;
- Receives incident data from private and public entities;
- Assists DOE, FERC, and the Department of Homeland Security (DHS) in analyzing event data to determine threats, vulnerabilities, trends and impacts for the sector, as well as interdependencies with other critical infrastructures (this includes integration with the DHS National Cybersecurity and Communications Integration Center (NCCIC));

[2] See https://www.esisac.com/.

- Analyzes incident data and prepares reports based on subject matter expertise in security and the BPS;
- Shares threat alerts, warnings, advisories, notices, and vulnerability assessments with the industry;
- Works with other ISACs to share information and provide assistance during actual or potential sector disruptions whether caused by intentional, accidental, or natural events;
- Develops and maintains an awareness of private and governmental infrastructure interdependencies;
- Provides an electronic, secure capability for the E-ISAC participants to exchange and share information on all threats to defend critical infrastructure;
- Participates in government critical infrastructure exercises; and
- Conducts outreach to educate and inform the electricity sector.

In addition to these activities and services, the E-ISAC has partnered with DOE on the Cybersecurity Risk Information Sharing Program (CRISP). Managed by the E-ISAC, CRISP uses innovative technology and leverages DOE's analytical capabilities. 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.

NERC Alerts

NERC also employs an alert system designed to provide concise, actionable security information to the electricity industry. NERC staff with appropriate security clearances often work with cleared personnel from federal agencies to communicate unclassified sensitive information to the industry in the form of NERC Alerts. As defined in NERC's Rules of Procedure, 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 41 cyber-related alerts (37 Industry Advisories and 4 Recommendations to Industry). Those alerts covered items such as Sabotage events, Aurora, Stuxnet, Night Dragon, and the reporting of suspicious activity. In 2016, NERC issued two Level Two alerts – the first related to the cyber security event in Ukraine and another concerning distributed denial of service attacks involving compromised Internet of Things[3] devices. Responses to alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders.

The NERC alert system is working well. It is understood by industry, handles sensitive information, and communicates this information in an expedited manner. The information needed to develop the alert is managed in a confidential manner. Information sharing through the E-ISAC is the greatest asset we have to combat emerging threats to cyber security and help ensure the reliability of the BPS.

GridEx

Consistent with our mission to promote a strong learning environment, NERC hosts a biennial grid security exercise – GridEx – which simulates widespread, coordinated cyber and physical attacks on critical electric infrastructure. Led by the E-ISAC, NERC conducted GridEx III on November 18–19, 2015.[4] GridEx III was the largest geographically distributed grid security exercise to date. GridEx III consisted of a two-day distributed play exercise and a separate

[3] 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.

[4] For more information on GridEx III, including a summary of results, see "Grid Security Exercise, GridEx III Report," March 2016, at: http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf.

executive tabletop session featuring 32 industry executives and senior officials from federal and state governments. All told, more than 4,400 individuals from 364 industry, law enforcement and government organizations across North America participated in GridEx III.

The objectives of GridEx III were to:

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

GridEx III provided participants with the opportunity to exercise their incident response procedures during large-scale security events affecting North America's electricity system. The large-scale cyber and physical attack scenario was designed to overwhelm even the most prepared organizations. Participating organizations were encouraged to identify their own lessons learned and share them with NERC. NERC used this input to develop observations and propose recommendations to help the electricity industry enhance the security and reliability of North America's BPS. Planning for GridEx IV in November 2017 is well underway.

GridSecCon

Consistent with promoting a learning environment and information exchange, NERC hosts the annual Grid Security Conference (GridSecCon). This widely attended conference brings together cybersecurity and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity sector. 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 security best-practice discussions on reliability concerns, risk mitigation, and physical security and cybersecurity threat awareness.

Ukraine

Cyber attacks on three distribution utilities in Ukraine on December 23, 2015, garnered significant attention. The Ukrainian incidents affected up to 225,000 customers in three distribution-level service territories and lasted for several hours.[5] A team from the United States, which included experts from the Department of Energy (DOE), the Department of Homeland Security (DHS), the Federal Bureau of Investigation and NERC, assisted the government of Ukraine in gaining more insight into the event.[6] The events in Ukraine are a reminder that cyber threats are real and that constant vigilance is needed to protect the reliability of the North American

[5] "Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case," SANS Industrial Control Systems and E-ISAC, March 18, 2016.
[6] See ICS-CERT report at https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

grid. At the same time, it is important to note that the operational and technical aspects of the North American BPS are different from those of the Ukrainian system. Other differences include the U.S. industry's mandatory and enforceable cyber security standards, including security management controls and authorized personnel and training controls; network segmentation; and the use of licensed anti-virus software, among other things.

Conclusion

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 diverse strategies utilizing robust CIP standards, situational awareness, information sharing with industry and government, and strong public private partnerships. NERC remains keenly focused on our mission to assure reliability of the BPS, which is inextricably tied to grid security.