NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Testimony of Gerry Cauley, President and Chief Executive Officer,
North American Electric Reliability Corporation

House Transportation and Infrastructure Committee
Subcommittee on Economic Development, Public Buildings, and Emergency Management

April 14, 2016

Introduction

Good morning Chairman Barletta, Ranking Member Carson, 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 reliability of the bulk-power system (BPS) in North America.

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. Therefore, assuring reliability, mitigating risks and preparing for recovery and restoration of the BPS following a loss of service is a vital concern.

My testimony discusses how NERC uses a range of tools to address key reliability challenges facing the BPS today. Given the subcommittee's interest in recovery efforts following a grid emergency, I will also discuss our biennial grid security exercise – a forward-looking initiative which helps industry and other stakeholders prepare for managing BPS security events. I welcome this opportunity to discuss these topics with the subcommittee.

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, FERC certified NERC as the Electric Reliability Organization 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 bulk power system through system awareness; and educates, trains, and certifies

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

industry personnel. Through the Electricity Information Sharing and Analysis Center (E-ISAC), NERC performs a critical role in real-time situational awareness and information sharing to protect the electricity industry's critical infrastructure against vulnerabilities. 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.

Reliability & Security Challenges

To assure the reliability and security of the North American grid, we must remain focused on emerging trends and the changing risk landscape, which ranges from conventional risks, such as extreme weather and equipment failures, to new and emerging risks in the security arena.

Physical Security Threats – Among other events, an April 2013 attack against a substation in California raised concerns about physical attacks on critical electric infrastructure. It is important to note the attack did not result in a power outage; in fact, no customer lost service. Nevertheless, the incident is a reminder of the vulnerabilities of our BPS and while rare, demonstrates that attacks are possible and have the potential to cause significant damage to assets and disrupt customer service. NERC's physical security standard – CIP-014-1 – requires users, owners and operators of bulk power system facilities to conduct a risk assessment to identify critical facilities and then develop and implement security plans to protect against attacks on those facilities. [1]

Cybersecurity Threats – In the Energy Policy Act of 2005, Congress anticipated the emerging cybersecurity threat by defining reliability standards to be developed by the ERO to include cybersecurity protection.[2] Since 2007, NERC has updated its standards to reflect the changing cybersecurity landscape. The fifth version of NERC's Critical Infrastructure Protection (CIP) cybersecurity standards will become effective on July 1 of this year. CIP Version 5 requires that all cyber assets must now be categorized as Low, Medium, or High Impact assets. The revised standards also include new requirements with new cybersecurity controls to address emerging cyber threats. In addition, CIP Version 5 uses a risk-based approach to implementing appropriate and changing technologies. That is, rather than specifying how to implement a requirement, the revised requirements specify the risk-based result that must be achieved, which enables industry to implement new and emerging technologies to address the risk. NERC is working with industry on the transition to this new standard, which is one of the most comprehensive, risk-based standards ever mandated. Today, the electric sector (along with nuclear) remains the only critical infrastructure sector subject to mandatory, enforceable cybersecurity standards.

Cyber attacks on three distribution utilities in Ukraine on December 23, 2015 has garnered significant attention. The Ukrainian incidents affected up to 225,000 customers in three distribution-level service territories and lasted for several hours.[3] A team from the United States, which included experts

[1] Federal Power Act, Sec. 215(a)(3).
[2] Federal Power Act, Sec. 215(a)(3).
[3] "Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case," SANS Industrial Control Systems and E-ISAC, March 18, 2016.

from the Department of Energy (DOE), the Department of Homeland Security (DHS), the FBI and NERC, assisted the government of Ukraine in gaining more insight into the event.[4] 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 grid. At the same time, it is important to note that the operational and technical aspects of the North American bulk power system 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.

The Changing Resource Mix/Essential Reliability Services – NERC must anticipate risks before they manifest as threats to reliability. For example, NERC is working with industry, regulators, and policymakers to assure reliability during a period of rapid transformation in the sources of energy used to produce electricity. Part of this effort includes two recent reports detailing the need to maintain essential reliability services.[5] ERS include frequency response, ramping capability, and voltage support, all of which are needed to assure that the grid remains balanced and able to respond and deliver electricity where it is needed when it is needed. The BPS is undergoing a broad transformation with retirements of coal units and some nuclear units, and additions of resources fueled by natural gas, wind, and solar. Distributed generation, energy efficiency, and demand response are also changing the way in which the grid is called upon to meet electricity demand. Regulations such as the Environmental Protection Agency's Clean Power Plan have the potential to hasten the transformation of the electric system. As this trend continues, it is critical for new resources to provide ERS. For more information on ERS, NERC has developed three videos designed to inform a general audience about the importance of these resources.[6]

FERC/NERC/Regional Entity Joint Review of Restoration and Recovery Plans – In January 2016, NERC published a joint report with FERC and NERC Regional Entities reviewing restoration and recovery plans of nine entities with significant bulk power grid responsibilities.[7] The objective of the review was to assess and verify the electric utility industry's bulk power system recovery and restoration planning, and to test the efficacy of related Reliability Standards in maintaining and advancing reliability in that respect. Overall, the joint staff review team found that the participants have system restoration plans to be thorough and highly-detailed. The reviewed plans require identification and testing of blackstart resources, identification of primary and alternate cranking paths, and periodic training and drilling on the restoration process under a variety of outage scenarios. Likewise, the joint staff review team found that participants had extensive cyber security incident response and recovery plans for critical cyber assets covering the majority of the response and recovery stages. In addition, the team observed that each participant has full time personnel dedicated to the roles and responsibilities defined in their respective

[4] See ICS-CERT report at https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[5] "Essential Reliability Services Task Force Measures Framework Report," NERC, November 2015.
See also "Reliability Considerations for Clean Power Plan Development," NERC, January 2016.

[6] See NERC ERS videos at https://vimeopro.com/nerclearning/erstf-1.

[7] "Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans," FERC/NERC/Regional Entities, January 2016, http://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf.

response and recovery plans. The joint staff review team identified several opportunities for improving system restoration and cyber incident response and recovery planning and readiness and further work will be done to follow up on the reports recommendations.

Electricity Information Sharing and Analysis Center

Mandatory and enforceable Reliability Standards are an important foundation of the complex endeavor to assure grid reliability. NERC employs other tools to help address new and emerging threats. Information-sharing through the NERC-operated E-ISAC[8] is one such tool.

The E-ISAC establishes situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely, reliable, and secure information exchange. The E-ISAC, in collaboration with DOE and the Electricity Sector Coordinating Council (ESCC),[9] 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:

- 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 member companies, as required;
- Issues alerts to industry ranging from advisory notices to essential actions requiring recipients to respond as defined in the alert;[10]
- Provides and shares campaign analysis, which includes capturing, correlating, trending data for historical analysis, and sharing that information within the sector;
- Receives incident data from private and public entities;
- Assists DOE, FERC, and 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));
- Analyzes incident data and prepares reports based on subject matter expertise in security and the bulk power system;
- 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;

[8] https://www.esisac.com/.
[9] See ESCC website at http://www.electricitysubsector.org/.
[10] http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx.

- 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.

GridEx III

Led by the E-ISAC, NERC conducted its third biennial grid security and emergency response exercise, GridEx III, on November 18–19, 2015.[11] GridEx III was the largest geographically distributed grid security exercise to date. GridEx III consisted of a two-day distributed play exercise (a simulated cyber and physical attack) and a separate 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.

Distributed Play Results

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, including:

- *Coordinated Response and Communication*. GridEx III highlighted the importance of well-coordinated communications. NERC recommended that organizations should review documentation that describes their internal information sharing processes in the context of a large-scale event and exercise these communication capabilities.

- *Reporting Mechanisms*. GridEx III participants observed that some aspects of the industry's information sharing and reporting tools are redundant, time-consuming to use, and provide no feedback mechanism to those who most need the information. NERC recommended that

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

organizations should review the tools and reporting processes in use to identify opportunities to improve the efficiency and efficacy of the information-sharing process.

- *Active Participation of Operations Management, Support Staff, and System Operators*. GridEx III succeeded in providing exercise scenarios that linked the physical and cyber attacks with how system operators would respond to mitigate the impact of these attacks on bulk power system reliability. NERC recommended that future GridEx exercises should continue to include scenarios that prompt operations management, support staff, and field operations to interact with cyber and physical security personnel. NERC also identified the essential role of reliability coordinators in designing future GridEx exercises to reflect local conditions and provide for effective coordination of generation, transmission and system operations in the context of cyber and physical security events.

- *E-ISAC Information Sharing*. Participants observed that the E-ISAC portal should be enhanced for real-time urgent communication with portal members. Participants observed that information was quickly buried within the portal, making it become difficult to highlight important information. NERC recommended that the E-ISAC should continue to enhance the E-ISAC portal to support real-time, searchable, urgent communication and collaboration with portal members.

- *Introduction of New Exercise Tools.* While new exercise tools enhanced the exercise, there is room for continued improvement. Prior to the next exercise, functionality and volume/capacity tests should be performed.

- *Advance Exercise Planning Timelines.* Planning for the next GridEx exercise should begin earlier than GridEx III to provide organizations with more time to conduct their own planning and training activities. NERC should develop a firm delivery schedule with stakeholders, including major planning milestones, and tool development and testing at the outset of exercise planning. Future GridEx exercises should continue to provide opportunities for organizations to customize their scenario injects provided they are consistent with and support the overall NERC scenario as coordinated with their Reliability Coordinator.

- *After-Action Survey and Lessons Learned.* During the early stages of the GridEx III planning process, NERC developed a set of metrics to assess the success of the exercise that included the questions in the after action survey. Lessons learned reports that were submitted to NERC by participating organizations provided valuable input, but a greater number of reports would provide a more complete and representative set of lessons learned. The NERC planning team should consult with participating active organizations to understand any reluctance to share lessons learned and identify ways to increase the response rate.

Executive Tabletop Results

The executive tabletop engaged senior leaders in a robust discussion of the policy issues, decisions, and actions needed to respond to a major grid disruption caused by simulated physical and cyber attacks. Participants identified security and reliability challenges and opportunities to improve prevention, response, and recovery strategies. The discussion centered on three key areas: unity of messaging, unity of effort, and extraordinary measures.

Unity of Messaging. Participants explored how industry and government assess a crisis event, and receive and share information with each other and the public. Managing the challenges and opportunities related to social media was of particular interest.

Unity of Effort. While both industry and government have considerable resources at the ready to respond to crisis events, participants considered how to improve coordination during severe emergency situations. Industry needs to coordinate with local law enforcement to identify and assess the physical risks to electricity facilities and workers. Unlike how industry responds to major storms through mutual assistance, industry's capability to analyze malware is limited and would require expertise likely available from software suppliers, control system vendors, or government resources.

Extraordinary Measures. The industry operates within a regulatory framework designed within normal planning and operating criteria. Participants considered regulatory and legislative needs, as well as extraordinary government support, that could enhance timely and effective recovery under extreme circumstances that clearly exceed normal criteria.

The following summarizes additional key findings from the executive tabletop:

- *Establish Priorities for Restoring Electricity Service*. When restoring power following a large-scale outage, utilities' first priorities focus on supplying electricity to re-start generation and energize transmission and distribution lines and equipment. Second priorities include "lifeline" customers such as communications, oil and gas, water supply/treatment and hospitals.

- *Simplify Electricity System Operation Under Emergency Conditions*. North America's electricity system is operated by highly trained staff using sophisticated technology systems to forecast load, monitor electricity flows, dispatch generation, remotely operate equipment, and administer markets. In the event that these normal processes are disrupted, it may be possible to simplify how the electricity system is operated to provide basic service but at reduced levels of reliability and less economically.

- *Consider Mechanisms to Prevent Financial Defaults*. Utilities will need unprecedented levels of financial resources in order to restore their facilities and eventually resume normal operations.

- *Manage Personal and Corporate Liability Risks*. North America's bulk power system is designed and operated to meet extensive legal and regulatory requirements (e.g., environmental, safety, financial, labor, commercial). Some of these requirements may delay or prevent restoration during a large-scale event.

Conclusion

As our economy becomes increasingly electrified, and as we become ever more dependent upon electric infrastructure, the reliability of the BPS becomes ever more important. The North American BPS is reliable and resilient. A strong and effective regime is in place to assure reliability. However, given the evolving threats to the BPS, we must remain vigilant. Grid Ex III showed that there is more that we can and should do to be better positioned to plan for and respond to a disruption of service upon which we all depend. This is a big job that involves everyone at the table today and many more.

I appreciate the opportunity to discuss NERC's role in assuring reliability and protecting the grid from physical and cyber threats, and would be pleased to answer any questions.