NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Comments of the North American Electric Reliability Corporation
to the National Institute of Standards and Technology, U.S. Department of Commerce

"Information on Current and Future States of Cybersecurity in the Digital Economy"
(Docket Number: 160725650-6650-01)

September 9, 2016

Executive Summary

As the Electric Reliability Organization ("ERO"), the North American Electric Reliability Corporation ("NERC") has statutory responsibility to assure reliability of the bulk power system ("BPS"). The cybersecurity threat is dynamic and ever-evolving. Managing this risk through a variety of measures is essential to assuring reliability. Among many strategies to address cybersecurity, NERC operates the Electricity Information Sharing and Analysis Center ("E-ISAC"), which serves as the principal portal for sharing security information between government and the electric power sector. NERC develops and enforces mandatory critical infrastructure protection standards for the electric sector. NERC also conducts numerous training and education efforts, including the Grid Security Conference and GridEX. Given NERC's expertise, NERC appreciates the opportunity comment on this effort by the National Institute of Standards and Technology ("NIST") and offer our assistance to work with the Cybersecurity Commission as they address this important subject. NERC's comments address the following topics:

Information Sharing and Coordination – Information sharing between government and industry is an essential element of any cybersecurity protection strategy. Government and the private sector should continue efforts to strengthen relationships with Information Sharing and Analysis Centers such as the E-ISAC. As sharing procedures continue to evolve, it is important to preserve existing relationships and avoid barriers to robust information sharing.

Public-Private Partnerships/Technology – NERC is a member of the steering committee of the Electric Subsector Coordinating Council ("ESCC"). The ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. Policies should continue to support this important public-private partnership.

The E-ISAC manages the Cybersecurity Risk Information Sharing Program ("CRISP"), an innovative public-private partnership between the Department of Energy ("DOE"), NERC, and the electric power industry to promote rapid sharing and analysis of cybersecurity information. CRISP's technology platform was initially developed by DOE. CRISP is an example of an effective public-private partnership commercializing technology that was initially developed by the federal government.

1325 G Street NW Suite 600
Washington, DC 20005
202-400-3000 | www.nerc.com

Critical Infrastructure Protection Standards – The electric power sector is subject to mandatory Reliability Standards, including standards addressing critical infrastructure protection. These standards provide a common cyber and physical foundation for owners and operators of the BPS. Reliability Standards are complementary to existing cybersecurity guidance such as the NIST risk management framework. Any new policies should avoid duplication or conflict with existing Reliability Standards.

Introduction

NERC is pleased to provide these comments to assist NIST in supporting the Commission on Enhancing National Cybersecurity ("Cybersecurity Commission").

NERC is a private non-profit corporation with statutory responsibility to assure reliability of the BPS. As the ERO for North America, 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.[1] 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. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

Government-Private Sector Coordination and Cooperation on Cybersecurity

Due to the dynamic and constantly evolving nature of the cyber threat, robust information sharing is an essential element of any cybersecurity strategy. NERC operates the E-ISAC,[2] which serves as the main secure information sharing portal for the electricity sector. NERC's E-ISAC provides situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely, reliable, and secure information exchange. Government and the private sector should continue efforts to strengthen relationships with Information Sharing and Analysis Centers. As sharing procedures continue to evolve, it is important to preserve existing relationships and avoid barriers to robust information sharing.

The E-ISAC gathers information from electricity industry participants across North America about security-related events, disturbances, and off-normal occurrences within the electricity subsector and shares that information with other electricity industry participants, key governmental entities (including Canada and Mexico), and cross-sector partners. The E-ISAC works routinely with government at all levels, including classified levels, on numerous security topics. The E-ISAC has cleared staff analysts who work with government analysts on classified information sharing. Governmental entities and cross-sector partners also provide the E-ISAC with information regarding risks, threats, and warnings that the E-ISAC

[1] 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, the Federal Energy Regulatory Commission certified NERC as the Electric Reliability Organization on July 20, 2006.

[2] NERC's E-ISAC webpage is available at the following link: https://www.esisac.com/.

disseminates throughout the electricity subsector. Two-way information sharing is critical because it allows the E-ISAC to help industry identify emerging trends and to provide an early warning, particularly in today's ever-changing security environment.

The E-ISAC uses a variety of tools, programs, and activities to enhance security, such as a secure web portal, alerts, exercises, training and education. The E-ISAC portal allows the E-ISAC to reach thousands of industry members and hundreds of organizations in the industry and is the mechanism for industry and government to contact E-ISAC staff with questions, concerns, and security-related information in a secure manner. The data received from industry members and partners helps the E-ISAC create timely, relevant, and actionable documents. As a result, NERC continues to grow the E-ISAC's capabilities by enhancing the E-ISAC's private, secure portal to receive voluntary reports from industry members, and, working with various organizations (both industry and government), to obtain the data and mechanisms necessary to conduct these information sharing activities. Some of the products the E-ISAC develops include daily, weekly, and monthly reports; incident bulletins; and issue-specific assessments. E-ISAC staff also advises the NERC Bulk Power System Awareness team on the issuance of NERC Alerts regarding cyber and physical security vulnerabilities.

Public-Private Partnerships/Technology

The discussion below reviews some of the ways NERC forges public-private partnerships and employs technology to advance cybersecurity protection.

Electric Sector Coordinating Council – NERC is a member of the steering committee of the Electric Subsector Coordinating Council ("ESCC").[3] The ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. Policies should continue to support this important public-private partnership.

Cybersecurity Risk Information Sharing Program – The Cybersecurity Risk Information Sharing Program ("CRISP") is a public-private partnership, cofounded by the U.S. Department of Energy ("DOE") and NERC, and managed by the E-ISAC, that facilitates the exchange of detailed cybersecurity information among industry, the E-ISAC, DOE, and Pacific Northwest National Laboratory ("PNNL"). The program facilitates information sharing and enables owners and operators to better protect their networks from sophisticated cyber threats. The underlying technology for CRISP was initially developed by DOE and deployed across the DOE networks more than 10 years ago.

Participation in the program is voluntary and enables owners and operators to better protect their networks from sophisticated cyber threats. The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information.

[3] ESCC's webpage is available at: http://www.electricitysubsector.org/.

CRISP information helps support development of situational awareness tools to enhance the sector's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources.

GridEx – Led by the E-ISAC, NERC conducted its third biennial grid security and emergency response exercise, 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 (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.

Grid Security Conference – NERC's annual Grid Security Conference ("GridSecCon") 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 sub-sector.[5] GridSecCon promotes reliability through training and education, delivers cutting-edge discussions on security threats, and informs industry of best-practices.

Critical Infrastructure Protection Standards

The electric sector is subject to mandatory Reliability Standards, including standards addressing critical infrastructure protection. These standards provide a common foundation for the BPS to address security and are complementary to non-regulatory strategies discussed above.

Since 2008, NERC has updated its Reliability Standards to reflect the changing cybersecurity landscape. On November 22, 2013, the Federal Energy Regulatory Commission ("FERC") approved a comprehensive suite of cybersecurity standards, referred to as the Critical Infrastructure Protection Version 5 standards ("CIP standards") which requires that all cyber assets must now be categorized as Low, Medium, or High Impact assets.[6] The revised standards include 12 new requirements with new cybersecurity controls to address emerging cyber threats.[7] In addition, the CIP standards remove technology-specific requirements by replacing them with a risk-based approach to implementing appropriate and changing technologies. 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.

Although the E-ISAC relies upon information that is shared voluntarily, the NERC CIP standards do require timely reporting of certain cybersecurity incidents to the E-ISAC[8] from a broad range of entities. Initial

[4] 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.
[5] For more information on GridSecCon, see http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridSecCon.aspx.
[6] 145 FERC ¶61,160 (November 22, 2013) (Order No. 791).
[7] The CIP standards are available at the following link: http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States.
[8] See CIP-008-5, Requirement 1.

notification must be made to the E-ISAC within one hour from a determination of a reportable cybersecurity incident.

DOE also requires electric sector reporting of cyber information. The "Electric Emergency Incident and Disturbance Report"[9] (DOE Form OE-417) collects information on electric incidents and emergencies, including events that are cyber-related. Depending on the nature of the attack or suspected attack, cyber incidents must be reported within one or ten hours. So as to avoid unnecessary burden on industry or duplication of effort, reporting entities may provide information through existing sharing procedures such as those through DOE or the E-ISAC.

In 2011, the General Accounting Office ("GAO") reviewed cybersecurity guidance for a variety of critical infrastructure sectors, including the electricity subsector.[10] GAO's review (of what was then Version 3 of the CIP standards) found that NERC's CIP standards are substantially similar to the NIST risk management framework.[11] As sharing procedures continue to evolve, it is important to preserve existing relationships and avoid barriers to robust information sharing. NERC seeks to ensure that any new initiatives by the Cybersecurity Commission avoid duplication or conflict with NERC standards, and, as has been the goal in the past, are complementary of respective missions.

Conclusion

NERC employs a variety of tools to promote critical infrastructure protection in the BPS. These include voluntary information sharing, public private-partnerships, and mandatory standards. As the Cybersecurity Commission continues its valuable work, it is important to recognize those initiatives and regulatory requirements that are working effectively so as to ensure that any new policies complement these measures. Given NERC's expertise in this area, NERC offers its assistance to work with the Cybersecurity Commission as they address this important subject. Again, NERC appreciates the opportunity to respond to this Request for Information.

[9] See DOE, Office of Electricity Delivery and Energy Reliability, "Electric Disturbance Events."
[10] "Critical Infrastructure Protection – Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use," U.S. Government Accountability Office, December 2011, GAO-12-92.
[11] Ibid, 35-36.