NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

National Institute of Standards and Technology Request for Comments North American Electric Reliability Corporation Response – December 13, 2013

Request for Comments Overview

This paper constitutes the North American Electric Reliability Corporation's (NERC) responses to the National Institute of Standards and Technology's (NIST) notice and request for comments on the preliminary version of the Cybersecurity Framework (Docket Number 130909789–3789–01), Fed. Reg. Vol. 78, No. 209 (October 29, 2013) at pp. 64478. NIST developed the preliminary Framework using information collected through open public workshops and the Request for Information (RFI) that was published in the Federal Register (Docket Number 130208119–3119–01), Fed. Reg. Vol. 78, No. 38 (February 26, 2013) at pp. 13024.

NERC's mission is to ensure the reliability of the North American Bulk Power System (BPS). NERC is the electric reliability organization (ERO) certified by the Federal Energy Regulatory Commission (FERC) to establish and enforce Reliability Standards for the BPS within the United States in accordance with Section 215 of the Federal Power Act enacted by the Energy Policy Act of 2005. NERC's Reliability Standards are mandatory and enforceable within the United States for the BPS and include Critical Infrastructure Protection (CIP) standards. The bulk power industry has the largest collection of collaboratively developed, mandatory and enforceable standards of any critical infrastructure sector. NERC develops and enforces Reliability Standards to secure the BPS; assesses adequacy annually via a 10-year forecast, and summer and winter forecasts; monitors the BPS; and educates, trains, and certifies industry personnel. In addition, NERC addresses security issues from both a physical security perspective, as well as a cybersecurity perspective. NERC engages with government and industry partners on threats, vulnerabilities, and mitigation strategies. ERO activities in Canada related to the reliability of the BPS are recognized and overseen by the appropriate governmental authorities in that country.

The BPS is highly interconnected, and the owners and operators are highly interdependent in their reliable operation of the grid. The grid is a single, very large machine. Disturbances and off-normal events at one location on the grid can have serious consequences at other, far-removed locations, even crossing international boundaries. At the same time, the asset owners and operators of the electricity industry comprise a numerous and widely diverse group, in terms of size, ownership, business model, and footprint. Within the United States, there are approximately 200 shareholder-owned utilities, 800 electric cooperatives, and more than 2,000 government-owned utilities. The largest may serve several millions of customers and have a footprint that spans several states. The smallest may serve only a few hundred

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

customers in a single municipality. Some entities are vertically integrated utilities that own and operate generation, transmission, and distribution assets. Other entities own no assets, but they have operating control over the transmission assets owned by third party entities, in a number of states. Some entities own and operate only transmission assets, while other entities may own or operate only generation assets.

The Preliminary Cybersecurity Framework

NERC believes the Cybersecurity Framework should provide a baseline cross-sector approach that, along with existing efforts, will further assist organizations in assessing and managing cyber risks. The Cybersecurity Framework should recognize existing efforts as equally effective measures to assist organizations in assessing and managing cyber risks, and it should encourage and provide incentives to entities to employ measures that go beyond those in the Framework.

Areas for Consideration

While NERC believes the Framework is a good starting point for organizations to initiate or bolster cybersecurity risk management activities, NIST and the Department of Homeland Security (DHS) should consider addressing the following areas before finalizing this first version of the Framework.

Recognize Existing Standards and Activities. The Electricity Sub-sector is more advanced in its cybersecurity efforts, and has several means available to it to meet the goals of the Framework. Over the course of the Framework development, NERC and the Electricity Sub-sector have emphasized and reiterated to NIST and DHS the importance of recognizing existing standards and practices under which sectors and companies are already operating. In the current and future versions of the Framework, the Framework should not duplicate, replace, or conflict with existing standards or risk-management activities, particularly if these standards and activities exceed the baseline approach outlined in the Framework. In its current state, the Framework provides a baseline approach, but it does not adequately recognize the existing mandatory standards and activities.

NERC has established Reliability Standards and has undertaken other efforts such as developing policies and procedures to address risk, including cybersecurity risk. These efforts include:

- Mandatory and enforceable CIP Reliability Standards, applicable to certain BPS users, owners, and operators
- Electricity Sector Information Sharing and Analysis Center (ES-ISAC) activities, including issuing alerts and providing analysis related to cybersecurity concerns
- High-Impact Low-Frequency Task Force reports identifying recommendations for owners and operators with respect to addressing severe impact resilience, cyber attacks, spare equipment, and geomagnetic disruptions
- Grid Security Exercise (GridEx) I and GridEx II, the only distributed-play exercise series focused solely on the Electricity Sub-sector in North America

- Government partnership initiatives, including the DHS's National Level Exercise series and various cybersecurity forums and briefings with Canadian government agencies, as well as the White House–initiated, Department of Energy (DOE)-led Electricity Sub-sector Cybersecurity Capability Maturity Model (ES-C2M2)
- Electricity Sub-sector Cybersecurity Risk Management Process (RMP) Guideline, developed with DOE, NIST, NERC, and the sub-sector, which supports ongoing development and measurement of cybersecurity capabilities and entity risk within the sub-sector

Additionally, in 2012, NERC established the Reliability Issues Steering Committee (RISC) to consider various threats to reliability, including those threats associated with cybersecurity, and to allocate appropriate levels of resources to respond to those threats. In February 2013, the RISC recommended to NERC's Board of Trustees that it consider threats associated with cyber attacks one of NERC's top priorities. NERC's Board accepted this recommendation, and the RISC is now working with NERC's Critical Infrastructure Department staff to develop actionable strategic plans for dealing with cyber attacks.

NERC's current risk management activities are mature and continue to evolve, and should be recognized as equally effective measures and as efforts that go beyond the Framework's baseline approach.

Identify Incentives Early. Throughout the Framework development process, NIST and DHS discussed the concept of incentives to encourage organizations to use the Framework. Cybersecurity insurance is one incentive that NIST, DHS, and the private sector have discussed extensively. These incentives need greater clarity and definition. NIST and DHS should clarify what organizations can do to achieve which incentives, and how, for example, insurance companies will acknowledge and accept these activities.

NIST and DHS should also clarify that companies or sectors that currently conduct risk management activities beyond those in the Framework (e.g., complying with mandatory NERC Reliability Standards, engaging in C2M2 activities), are eligible for incentives, and provide guidance on information needed to qualify and maintain the incentives.

Identifying early in the process what the incentives are and how organizations can benefit from them will not only provide clarity to the organizations on what activities they could employ, but would also encourage greater participation in risk management activities.

Keep the Framework Voluntary. The Framework was developed to reduce cyber risks to critical infrastructure. The Electricity Sub-sector—as well as several other sectors—already engages in significant cyber risk management activities. Mandating use or adoption of the Framework may conflict with, or create duplicative activities that may already be mandated by regulatory authorities, or are already in practice through Information Sharing and Analysis Centers or other information sharing organizations.

Sectors should work with their Sector Specific Agencies (SSA) to align priorities and resourcing to leverage existing vetted frameworks after identifying gaps in risk management assessments. The SSA should work closely with the Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) to facilitate support for the ISACs.

Respectfully submitted,

/s/ Rebecca J. Michael

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
charles.berardesco@nerc.net

Rebecca J. Michael
Associate General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
rebecca.michael@nerc.net

Counsel for North American Electric Reliability Corporation