UNITED STATES OF AMERICA
BEFORE THE
U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NIST SMART GRID CYBER SECURITY STRATEGY AND REQUIREMENTS (SECOND DRAFT NISTIR 7628)

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

June 2, 2010

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") is pleased to provide these comments in response to the National Institute of Standards and Technology's ("NIST") second draft of *Smart Grid Cyber Security Strategy and Requirements* ("NISTIR 7628 Second Draft").[1] NERC has been certified by the Federal Energy Regulatory Commission ("FERC" or the "Commission") as the "electric reliability organization" under Section 215 of the Federal Power Act[2] and is similarly recognized by applicable governmental authorities in Canada. Because NERC's mission is to ensure the reliability and security of the bulk power system in North America by, in part, developing and enforcing mandatory Reliability Standards, NERC's comments on the NISTIR 7628 Second Draft focus on the development by NIST of an overall cyber security strategy for the smart grid as it relates to the security of the bulk power system and NERC's mandatory Reliability Standards, and in particular, to NERC's Critical Infrastructure Protection ("CIP") Reliability Standards.

[1] *Smart Grid Cyber Security Strategy and Requirements, Draft NISTIR 7628*, National Institute of Standards and Technology, U.S. Department of Commerce, February 2010.

[2] *See* North American Electric Reliability Corporation, "Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing." 116 FERC ¶ 61,062 (July 20, 2006).

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to these comments may be addressed to the following:

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
Holly A Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

III. BACKGROUND

In February 2010, NIST released the NISTIR 7628 Second Draft, which updated the first *Smart Grid Cyber Security Strategy and Requirements* ("NISTIR 7628 First Draft") document released on September 25, 2009. NERC provided comments to NIST in response to the NISTIR 7628 First Draft on December 1, 2009.[3] The NISTIR 7628 Second Draft document outlines an overall cyber security strategy examining both domain-specific and common requirements. NERC also provided comments to NIST in response to the NIST Framework and Roadmap for Smart Grid Interoperability Standards document[4] on November 9, 2009.[5] NERC's comments on that document specifically focused on the development of voluntary interoperability standards as

[3] *See*, NERC December 1, 2009 Comments on NISTIR 7628 First Draft ("NERC December 1 Comments"). NERC's comments in response to the first draft of the Smart Grid Cyber Security Document can be found on NERC's website at the following link: http://www.nerc.com/files/NIST%20Smart%20Grid%20Comments%20on%20Cyber%20Security%20Strategy.pdf

[4] *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)*, Office of the National Coordinator for Smart Grid Interoperability, U.S. Department of Commerce, September 2009 ("Smart Grid Framework Document").

[5] NERC's comments in response to the Smart Grid Framework Document can be found on NERC's website at the following link: http://www.nerc.com/files/FinalNERCCommentsNIST_Smart_Grid_Framework_Document.pdf.

they relate to NERC's mandatory Reliability Standards, and in particular, to NERC CIP Reliability Standards.

In a Federal Register notice published on April 13, 2010, NIST summarized the public comments received in response to the NISTIR 7628 First Draft and requested comments by June 2, 2010. NERC is commenting herein on key points expressed in NERC's previous comments to the NISTIR 7628 First Draft that were not addressed in the NISTIR 7628 Second Draft, which serve to emphasize NERC's continued concern with these issues.

IV. DISCUSSION

I. NIST States that NERC CIP Reliability Standards are Mandatory for the Bulk Power System. In Fact, NERC's CIP Reliability Standards are Designed for Asset Owners and Operators, and not Equipment and Control System Designers, Manufacturers, and Integrators.

In the NISTIR 7628 Second Draft, NIST states that currently, only the NERC CIP Reliability Standards are mandatory for the bulk electric system. NERC agrees that the CIP standards were not designed to, nor are they intended to, reach beyond the reliability of the bulk electric system. As NERC noted in its comments on the NISTIR 7628 First Draft, the applicability of NERC-developed, FERC approved CIP Reliability Standards is limited to users, owners, and operators of the bulk power system in accordance with Section 215 of the Federal Power Act.[6] However, most smart grid technologies and applications will be applied at the customer and distribution system levels, which are not typically considered to be part of the bulk power system. Therefore, the aggregated impacts of these smart grid devices, from, for example, equipment and control system designers, manufacturers, and integrators on the bulk power system could be substantial.

[6] *See* NERC December 1 Comments at pp. 6-7 and pp. 15-17.

While the applicability of NERC-developed, FERC-approved, cybersecurity standards is limited to users, owners and operators of the bulk power system in accordance with Section 215 of the Federal Power Act, smart grid technologies and applications will reach into the distribution system. Smart grid devices will operate at positions within the grid that are not typically considered to be part of the bulk power system.

Therefore, if a threat to cyber security on the bulk power system could take place at the distribution end of the grid, such as on a smart grid home device, there may be a need to implement changes and or additions to NERC's CIP Reliability Standards based on new smart grid technologies and applications that will take into account bulk power system reliability impacts from both ends of the grid. In isolation these impacts are insignificant. But in aggregate, thousands of these devices failing or mal-operating in unison, or even operating in unison, can pose a distinctly difficult challenge to the reliability and security of the bulk power system. Additionally, NERC believes that with increasing interconnectedness of business and control systems resulting from smart grid technologies, there is a greater risk of access for potential attackers as more complex architectures and more accessible technologies are added in the form of neighborhood wireless networks and embedded devices outside of a user, owner, or operator of the bulk power system's control.

While the purpose of developing interoperability standards for the smart grid is to ensure that smart grid systems can freely exchange information without logical barriers, the NERC CIP Reliability Standards purposefully put barriers in place to protect the various elements that comprise the critical infrastructure assets of the bulk power system, including critical cyber assets, from malicious intrusion or attack. As such, NIST must recognize that its application of the NERC CIP Reliability Standards to the body of smart grid interoperability standards *will not* adequately protect cyber security of all components of the smart grid, such as smart grid distribution devices.

For example, NERC's CIP Reliability Standards do not specifically protect telecommunications systems or communication paths, which are important components of the smart grid. Additionally, NERC CIP Reliability Standards do not provide requirements for actual components, such as the requirement for device-to-device authentication. While the CIP Reliability Standards are designed to shape the behavior of asset owners and operators, they are not designed to shape the behavior of equipment and system designers, manufacturers, and integrators. The NERC CIP Reliability Standards apply to installed equipment and require security controls be applied to manage risk in the operation and maintenance of bulk power system cyber assets. The protection goals of the smart grid, on the other hand, are broader, and address component security, integrity of communications, privacy, and other cyber security considerations. Accordingly, NERC encourages NIST to integrate adequate cyber security protection at all levels (device, application, network and system) in the development of interoperability standards for the smart grid.

II. NIST Presents a Logical Interface Analysis and Characterizes them with the Smart Grid.

In the NISTIR 7628 Second Draft, NIST presents an analysis of the logical architecture and interfaces of the smart grid, which is useful in analyzing smart grid domains and actors and potential cyber security vulnerabilities. There are two areas of consideration NERC requests NIST to consider in its analysis to help ensure the reliability and security of the bulk power system as smart grid technologies and applications are developed. First, control systems and optimization systems need to work harmoniously, with reliability and security designed and present throughout. Second, NERC believes that category definitions for fully functional and

degraded modes of operation would be helpful to assess the security and reliability of the system. Each of these is discussed in greater detail below.

a. Control Systems and Optimization Systems Need to Work Harmoniously, with Reliability and Security Designed and Present Throughout.

NERC and NIST must carefully assess any potential cyber security impacts on the smart grid and the work that is required to ensure that potential cyber security risk is effectively managed in light of newly discovered cyber security vulnerabilities. Many smart grid users are just now considering the Supervisory Control and Data Acquisition ("SCADA") environment. Therefore, even if cyber security practices are working in the IT and telecommunications realm, a system more impervious to cyber attacks requires additional work in an integrated, embedded, system control and network environment.[7]

The bulk power system is made up of large amounts of system inertia, and existing control systems are used to manage a very large, nonlinear system. Cyber security strategy that works for one area (*e.g.*, IT or telecommunications) cannot be assumed to effectively be applied in a smart grid environment where new tools and equipment will be integrated to make up the smart grid, thereby potentially introducing new cyber security vulnerabilities on a regular basis.

Additionally, the bulk power system is operated by a complex system of systems. This complex system currently relies on delicately integrated control systems that have been refined over decades to provide highly reliable control of the bulk power system. While the smart grid may introduce new optimization systems that perform specific roles in achieving smart grid functions (*e.g.*, reduced energy use, optimization of assets, increased awareness), these new systems must also work near flawlessly with each other and legacy control systems. Meanwhile, new and advanced smart grid control systems will be introduced to improve reliability on the

[7] These concepts are discussed in more detail in NERC's December 1 Comments a pp. 11-12.

grid, and these control systems will need to function seamlessly with legacy systems and new optimization systems.

Therefore, because a common and overarching concern is cyber security for all systems on the grid and new systems being introduced as smart grid, designing and initially introducing such systems with robust cyber security features will support bulk power system reliability and be more cost-effective than integrating cyber security features after implementation.

b. Category Definitions for Fully Functional and Degraded Modes of Operation would be Helpful to Assess the Security/Reliability of the System.

Chapter Three of the NISTIR 7628 Second Draft provides an overview of NIST's Logical Interface Analysis and the security requirements that may impact the smart grid. While NERC believes the use cases provided in Chapter Three are useful because they help the industry consider potential concerns associated with the smart grid, the impacts analyzed miss an important point that should be examined. The category definitions should be looked at with what would be the core components of that category in the event of a system operating in a "fully capable" mode, a "degraded" mode, or a "not capable" mode. NERC discussed these concepts in more detail in its comments in response to the NISTIR 7628 First Draft.[8]

Additionally, some of the use cases analyzed in Chapter Three, while important, should not command a higher priority with respect to cyber security protection and recovery if they are not core components that drive the electric system. Accordingly, NERC recommends that the core components be clearly examined and separated from those components that merely provide optimization of the smart grid.

[8] *See* NERC's December 1 Comments at pp. 14-15.

III. NIST's Discussion Regarding Overall Risks to the Electric System: The Development of an Overall Cyber Security Strategy of the Smart Grid Includes Standards Required for the Integration for use by their Integrators.

NIST discussed the importance of interfaces in the NISTIR 7628 Second Draft and explains how these interfaces will come together to create the smart grid. NERC agrees that these interfaces are important, and recommends that interoperability standards be developed that apply directly to the integrators and the equipment being integrated to ensure that requirements are in place to support interconnection of one system to another. One method of achieving this is to consider developing standards that apply to the integration of smart grid systems for use by their integrators. NERC discusses these concepts in more detail in its response to the NISTIR 7628 First Draft.[9]

IV. The Energy Independence and Security Act Requires that Standards be Developed to Maintain a Reliable and Secure Infrastructure to Meet Future Demand and Growth. NERC Believes That the System Core Components Should be Designed to Maintain CORE Functions in the Event of a Cyber Security Incident—a Task that is Essential in Ensuring the Reliability and Security of the Smart Grid.

In Chapter Three of the NISTIR 7628 First and Second Drafts, NIST analyzes the interface diagrams for the six functional priority areas discussed in the Smart Grid Framework Document. While NIST's analysis is useful in examining some of the potential cyber security vulnerabilities of the smart grid, it does not adequately describe the impacts of a vulnerability on each interface in such a way that will allow the industry to adequately determine how to prioritize cyber security protection and recovery of the systems and parts that will make up the smart grid.

One suggested approach that will provide the industry with the information it needs to prioritize cyber security protection and recovery of the core components of the smart grid is to

[9] *See* NERC's December 1 Comments at pp. 8-10.

include in Chapter Three of NISTIR 7628 an examination of the core capabilities of the six functional areas explored. Because not all control systems are equal, and many system enhancements will enable grid optimization only, it is essential that the industry have a mechanism in place in which the core capabilities can be defined and separated from those parts of the smart grid that optimize the grid. While NERC supports an optimized grid, NERC believes it is more important that the industry have the capability to segment the essential core components of the smart grid so that in the event of a high risk or incident, the core components can be addressed first and preserved to maintain bulk power system reliability. Accordingly, it will be essential to distinguish between core components and optimization functions.[10]

NERC proposes two strategies for developing a cyber security framework for the smart grid:

1) In an organized and designed way, NIST and the industry need to develop a focus on response and recovery. While the first goal of a cyber security strategy should be on prevention, it also requires that a response and recovery strategy be developed in the event of a cyber attack on the electric system. More planning and investment is needed to develop response and recovery actions, while continuing to develop a strategy for prevention of a cyber security incident.

2) It is essential that those parts or equipment of the smart grid that optimize the system are separate from the core components of the smart grid. The core components are those components that are essential to enabling a functioning electric grid. Therefore, the core components of the smart grid must be understood so that, in the event of a cyber security incident on the grid, the core components can be recovered with minimal technology in a quick and efficient manner, ensuring bulk power system reliability. This attention on the core components of the smart grid will also help identify where response plan decisions and actions can be carried out to protect core functionality and/or quickly restore it.

While NERC believes the use cases provided in Chapter Three are useful because they help the industry consider potential concerns associated with the smart grid, the impacts analyzed must be looked at with what would be the core components of that category in the event of a system operating in various operating states. Additionally, the use cases analyzed in Chapter Three, while important, should not command a higher priority with respect to cyber security

[10] *See* NERC's December 1 Comments at pp. 18-21.

protection and recovery if they are not core components that drive the electric system. Accordingly, the core components should be clearly examined and separated from those components that merely provide optimization of the smart grid.

V. CONCLUSION

For the reasons stated above, NERC looks forward to working with NIST in developing a smart grid cyber security strategy that works collaboratively and in conjunction with NERC Reliability Standards. Additionally, because cyber security and reliability will be of paramount importance in the development of a smarter grid, NERC encourages NIST to develop an overall cyber security strategy for the smart grid that provides the tools necessary to analyze potential cyber security vulnerabilities of the smart grid on an ongoing basis so that the industry has the tools necessary to work collaboratively to ensure a safe and reliable grid.

Respectfully submitted,

/s/ Holly A. Hawkins

Gerald W Cauley
President and Chief Executive Officer
David N. Cook
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

June 2, 2010