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 ON NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS, RELEASE 1.0 (DRAFT)

Rick Sergel
President and Chief Executive Officer
David N. Cook
Vice President and General Counsel
Michael J. Assante
Vice President and Chief Security Officer
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

November 9, 2009

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 ("NIST") Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 ("Smart Grid Framework Document").[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 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 subject to FERC approval, NERC's comments on the Smart Grid Framework Document focus on the development by NIST of voluntary Interoperability Standards as they may relate to NERC's mandatory Reliability Standards, and in particular, to NERC Critical Infrastructure Protection ("CIP") Reliability Standards.

[1] 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").

[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:

Rick Sergel
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

The NIST Smart Grid Framework Document outlines the first phase of a three-phase plan for NIST to accelerate the identification of interoperability standards and develop a robust framework for the long-term evolution of standards related to Smart Grid. While most of the interoperability standards identified pertained to the technical requirements for the interoperability of equipment, the report also acknowledges NERC's Critical Infrastructure Protection ("CIP") CIP-002 through CIP-009 Reliability Standards as the only mandatory NERC Standards "directly relevant to Smart Grid."[3] It is on this basis that NERC hereby provides these comments to respond to the Smart Grid Framework Document.

[3] Smart Grid Framework Document at p. 78.

NIST also released a draft of a document entitled *Smart Grid Cyber Security Strategy and Requirements* ("Smart Grid Cyber Security Document") on September 25, 2009 containing an overall cyber security risk management framework and strategy for the Smart Grid. That document maps NERC's mandatory CIP Standards to similar cyber security documents from the Department of Homeland Security ("DHS"), the International Electrotechnical Commission ("IEC"), the American National Standards Institute ("ANSI") and others. NERC plans to provide comments to NIST on the Smart Grid Cyber Security Document by December 1, 2009.

On March 19, 2009, FERC issued a document entitled *Smart Grid Policy, Proposed Policy Statement and Action Plan Order* ("Proposed Policy Statement")[4] on which NERC provided comments. The Commission issued a Final Policy Statement on July 16, 2009,[5] which provided guidance regarding the development of a Smart Grid for the nation's electric transmission system, focusing on the development of key standards to achieve interoperability and functionality of Smart Grid systems and devices. While the Commission will ultimately be responsible for adopting "interoperability standards and protocols necessary to ensure smart-grid functionality and interoperability in the interstate transmission of electric power and in regional and wholesale electricity markets,"[6] NIST, in accordance with the Energy Independence and Security Act of 2007 ("EISA"), Section 1305(a), was directed "… to coordinate the advancement of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems."[7] NIST's Smart Grid Framework Document presents the results of the first of three phases of that project.

[4] Smart Grid Proposed Policy Statement and Action Plan, 126 FERC ¶ 61,253 (March 19, 2009), Docket No. PL09-4-000 ("FERC Proposed Policy Statement").
[5] Smart Grid Policy Statement, 128 FERC ¶ 61,060 (July 16, 2009), Docket No. PL09-4-000 ("FERC Policy Statement").
[6] FERC Proposed Policy Statement at P 1 n.3, citing to the Energy Independence and Security Act of 2007, Pub. L. No. 110-140, 121 Stat. 1492 (2007) ("EISA"), to be codified at 15 U.S.C. §17381(a).
[7] FERC Proposed Policy Statement at P 7 n.7, citing to EISA §1305(a).

Based on NERC's review of the Smart Grid Framework Document, there are three types of standards (either currently existing or to be developed) that NERC believes will be important to ensuring the successful operation, reliability and security of Smart Grid technologies. These standards are – Interoperability Standards, System Security Standards and Reliability Standards. Each is described below.

Interoperability Standards

The NIST Framework Document defines "Interoperability" as "[t]he capability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user. ... [t]hat is, different systems will be able to exchange meaningful, actionable information. The systems will share a common meaning of the exchanged information, and this information will elicit agreed-upon types of response. The reliability, fidelity, and security of information exchanges between and among Smart Grid systems must achieve requisite performance levels**."**[8] "Standards" are defined in the Smart Grid Framework Document as: "Specifications that establish the *fitness of a product for a particular use* or that define the *function and performance of a device or system.* Standards are key facilitators of compatibility. They define specifications for languages, communications protocols, data formats, linkages within and across systems, interfaces between software applications and between hardware devices, and much more. Standards must be robust enough so that they can be extended to accommodate future applications and technologies."[9]

For purposes of this document, NERC has referred to NIST's discussion of standards for the Smart Grid as "Interoperability Standards." NERC notes that the Interoperability Standards

[8] Smart Grid Framework Document at p. 11-12.
[9] *Id.* at p. 12.

proposed in the Smart Grid Framework Document appear to focus on components and applications, and in many cases do not directly address interoperability of networks and systems. That is, the Smart Grid Framework Document proposes Interoperability Standards that today are useful for component designers and manufacturers, but may not be adequate for system integrators and utilities to guide architectures and system properties. Standards developed for interoperability of networks and systems will also need to be carefully evaluated to ensure that no incompatibilities or conflicts are inadvertently created that could potentially adversely affect the reliability of the bulk power system.

System Security Standards

System security standards ("System Security Standards") refer to those standards that will apply to the technology and architecture of the system network and components that will collectively enable the functionality of Smart Grid technologies. According to FERC's Proposed Policy Statement, System Security Standards should address the following considerations: (1) the integrity of data communicated (whether the data is correct); (2) the authentication of the communications (whether the communication is between the intended Smart Grid device and an authorized device, network, or person); (3) the prevention of unauthorized modifications to Smart Grid networks and devices and the logging of all modifications made; (4) the physical protection of Smart Grid networks and devices; and (5) the potential impact of unauthorized use of these Smart Grid networks and devices on the bulk-power system.[10] Although there is no cited authority in the Smart Grid Framework Document, NERC believes it will be essential to address system security considerations to ensure that the standards for the design and integration of Smart Grid systems, networks and technologies do not conflict with or create unintended

[10] *Id.* at P 30.

reliability and security risks for the bulk power system. NERC will address this issue in more detail in its comments in response to NIST's Smart Grid Cyber Security Document, which will be sent to NIST by December 1, 2009.

NERC Reliability Standards

NERC Reliability Standards ("Reliability Standards") are the international standards that ensure reliability of the bulk power system. Through the Energy Policy Act of 2005,[11] Congress provided for the creation of an ERO, charged with developing and enforcing mandatory Reliability Standards in the United States, subject to Commission approval. NERC was certified by the Commission as the designated ERO on July 20, 2006.[12] NERC's role as the ERO is to develop, implement, and enforce mandatory Reliability Standards for the bulk power system, subject to Commission approval, in accordance with Section 215 of the Federal Power Act (the "Act" or the "FPA").[13] Section 215 requires that all users, owners and operators of the bulk power system in the United States be subject to the Commission-approved Reliability Standards. NERC-enforced, and Commission-approved Reliability Standards are designed to ensure the reliability of the bulk power system and typically apply to those entities that perform the planning, design, maintenance, and operation of facilities at the transmission and generation level.

While NERC understands that NIST's development of Interoperability Standards will help to implement devices and programs to enable the functionality of a Smart Grid, NERC's role with respect to this process is to specifically address whether new Reliability Standards, or

[11] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005) (codified at 16 U.S.C. §824o (2007)).
[12] *See* North American Electric Reliability Corporation, 116 FERC ¶61,062 (July 20, 2006)
[13] *See Id.*; citing to, FPA §§ 824, 824o.

modifications to existing mandatory Reliability Standards, will be necessary, to ensure the continued reliability of the bulk power system as new Smart Grid technologies and systems are developed and integrated with existing systems and networks.

IV. DISCUSSION

The title of the Smart Grid Framework Document suggests that this document is a roadmap for the development of Interoperability Standards to apply to the Smart Grid. However, the contents appear to be a "plan" for the development of Interoperability Standards rather than a roadmap as they do not provide a full complement of interoperability requirements now and into the future (*i.e.*, off-ramps, expected evolution). Rather, the Smart Grid Framework Document appears to be a compendium of high priority elements, each with its own plan and milestones. Although there are references to "reliability" throughout the document, these references are generally attributed to the reliability of Smart Grid devices and systems rather than the reliability of the bulk power system or electric distribution systems.

Accordingly, NERC's comments herein focus on suggested areas for NIST's further consideration in the development of Interoperabilty Standards for the Smart Grid. As discussed below, it will be vitally important for NIST Interoperability Standards to be developed in close coordination with NERC Reliability Standards to ensure the continued reliability of the bulk power system.

1. NIST's Proposed Interoperability Standards Must be Compatible with NERC Reliability Standards

Although the voluntary Interoperabilty Standards proposed by NIST are designed to achieve a different purpose from the NERC mandatory Reliability Standards, it is critical to the

continued reliability of the bulk power system that the two bodies of standards be compatible and complementary. The EISA has tasked NIST with the "responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems."[14] The Smart Grid Framework Document states that "[t]he Smart Grid is a very complex system of systems," and "[t]here needs to be a shared understanding of its major building blocks and how they inter-relate (an architectural reference model) in order to analyze use cases, identify interfaces for which interoperability standards are needed, and to develop a cyber security strategy."[15] In order to achieve this, Interoperabilty Standards will be required to address "how to" achieve interoperability of the Smart Grid (*e.g.* what type of equipment an entity must use to interoperate with other Smart Grid entities, and how that equipment will communicate with each other).

NERC Reliability Standards, on the other hand, deal with "what" should be done to ensure the reliability of the bulk power system. The definition of "Reliability Standard" as it appears in Section 39.1 of the Code of Federal Regulations is:

> "... a requirement to provide for reliable operation of the bulk power system, including without limiting the foregoing, requirements for the operation of existing bulk power system facilities, including cyber security protection, and including the design of planned additions or modifications to such facilities to the extent necessary for reliable operation of the bulk power system; but shall not include any requirement to enlarge bulk power system facilities or to construct new transmission capacity or generation capacity."

NERC, as an ANSI-accredited standards-setting body, is responsible for developing mandatory Reliability Standards for the reliability of the bulk power system. NERC's role as the ERO is to develop, implement, and enforce mandatory Reliability Standards for the bulk power system, subject to Commission approval, in accordance with Section 215 of the FPA.[16] Section

[14] EISA Title XIII, Section 1305.
[15] Smart Grid Framework Document at p. 5.
[16] 16 U.S.C. Section 824o.

215 requires that all users, owners and operators of the bulk power system in the United States comply with Commission-approved Reliability Standards, which are designed to ensure the reliability of the bulk power system and typically apply to entities that own, operate, and use facilities at the transmission and generation level. Additionally, Section 401.2 of the NERC Rules of Procedure provides that "[w]here required by applicable legislation, regulation, rule or agreement, all bulk power system owners, operators, and users, regional entities, and NERC, are required to comply with all approved NERC reliability standards at all times."[17]

Although NIST's voluntary Interoperability Standards and NERC's mandatory Reliability Standards are designed to serve fundamentally different purposes, it is essential that they be compatible and that no inadvertent conflicts arise that make it impossible for entities to be able to comply with both. An entity should be able to comply with both NERC Reliability Standards listed on Table 2 and NIST Interoperability Standards. Because Interoperability Standards will likely apply to equipment and systems that interface with the equipment and systems of bulk power system users, owners, or operators' equipment, and because these Interoperability Standards could become *de facto* mandatory standards that all Smart Grid technologies and systems will adopt, it will be important for NERC and NIST to coordinate on the development of the interoperability standards that affect the reliability and the security of the bulk power system.

NERC looks forward to working collaboratively with NIST in the development of Interoperabilty Standards that are compatible with NERC Reliability Standards.

[17] NERC's Rules of Procedure are available at: http://www.nerc.com/page.php?cid=1|8|169.

2. Cyber Security of the Smart Grid is a Top Priority; However Inclusion of the NERC CIP Standards Into the Interoperability Standards Will Not Ensure Complete Cyber Security Protection of Smart Grid Devices and May Have Unintended Consequences

In the Smart Grid Framework Document, NIST states that cyber security is a "critical priority," covering all aspects of reliable Smart Grid integration and deployment and should be a top priority.[18] While NERC agrees that cyber security is a top priority, NERC CIP Reliability Standards are not intended to reach beyond the reliability of the bulk power system. NERC therefore encourages NIST to use caution in applying NERC CIP Reliability Standards to the body of Interoperability Standards to ensure cyber security protection of Smart Grid devices.

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 FPA. Smart Grid technologies and applications will generally be applied at the customer and distribution system levels, which are not typically considered to be part of the bulk power system. However, the aggregated impacts of these Smart Grid devices on the bulk power system could be substantial.

While the purpose of developing Interoperability Standards 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 Interoperability Standards *will not* adequately protect cyber security of all components of the Smart Grid, such as Smart Grid distribution devices.

[18] *See* Smart Grid Framework Document at p. 7.

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 Reliability Standards apply to installed equipment and require security controls be applied to manage risk in the operation and maintenance of 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) for the Smart Grid in the development of a body of Interoperabilty Standards. While NERC CIP Reliability Standards provide for the reliable and safe operation of the bulk power system by preventing the unauthorized cyber and physical access to critical assets and critical cyber assets, there is a need to develop additional cyber security protection for distribution facilities in the development of Smart Grid Interoperability Standards to address, for example, security aspects of interoperability at the distribution level. Therefore, new Smart Grid system designs that can help manage cyber security risks must be explored to ensure that suitable reliability and security considerations are included in NIST's Interoperability Standards.

NERC intends to work closely with NIST through the Smart Grid Interoperabilty Panel and in other forums on the development of cyber security Interoperability Standards for Smart Grid technologies and their associated network and system architectures, with an eye toward

pass-through attacks (*i.e.* an attacker moving from a point in the system to other critical infrastructure systems) and aggregated impacts to the bulk power system. Additionally, NERC will provide more substantive comments in response to NIST's Smart Grid Cyber Security Document by December 1, 2009.

3. All Interoperability Standards Need to be Harmonized

In its textbox labeled "Guidance for Identifying Standards for Implementation," NIST presents a list of criteria for evaluating Interoperability Standards and emerging specifications.[19] In this list, NIST proposes that a standard or emerging specification be evaluated on "whether it is integrated and harmonized with complementing standards across the utility enterprise through the use of an industry architecture that documents key points of interoperability and interfaces."[20] NERC concurs that evaluating proposed Interoperability Standards against this criterion is a good practice and critical to the success of the NIST Interoperability Standards identification process. Although NIST states that this criterion "does not apply to every standard or specification listed in Tables 2 and 3," NERC asserts that this specific criterion be fully applicable to all of the proposed interoperability standards in those tables as it represents a fundamental attribute for system-wide interoperability and will ensure that all standards proposed to be included in the body of Interoperability Standards are compatible and complementary with each other.

[19] Smart Grid Framework Document at p. 46.
[20] Smart Grid Framework Document at p. 46.

V. CONCLUSION

For the reasons stated above, NERC looks forward to working with NIST in developing Interoperability Standards that work collaboratively and in conjunction with NERC Reliability Standards, recognizing that new or modified NERC Reliability Standards may also be necessary to integrate Smart Grid technologies based on their impact on bulk power system reliability. Additionally, because cyber security and reliability will be of paramount importance in the development of a smarter grid, NERC encourages NIST to develop cyber security Interoperability Standards that relate to Smart Grid technologies and systems.

Respectfully submitted,

/s/ Holly A. Hawkins

Rick Sergel
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