UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

SMART GRID INTEROPERABILITY STANDARDS	**)** **)** **)**	**Docket No. RM11-2-000**

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION ON THE JANUARY 31, 2011 TECHNICAL CONFERENCE

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior 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

Holly A. Hawkins
Assistant General Counsel
Willie L. Phillips
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
holly.hawkins@nerc.net
willie.phillips@nerc.net

April 8, 2011

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[1] hereby provides these comments on the Federal Energy Regulatory Commission's ("FERC" or "Commission") January 31, 2011 technical conference regarding smart grid interoperability standards. On February 16, 2011, in light of the discussion at the technical conference, FERC issued a Supplemental Notice Requesting Comments ("February Supplemental Notice") on a series of questions.[2] On March 2, 2011, the Commission issued a Notice of Extension of Time, granting an extension until no later than April 8, 2011, to submit comments in this proceeding.

Because NERC's mission, as the FERC-designated Electric Reliability Organization ("ERO"),[3] is to ensure the reliability of the bulk power system in North America by, in part, developing and enforcing mandatory Reliability Standards, NERC's comments herein focus primarily on three questions related to the impact of the smart grid interoperability standards on reliability.

[1] FERC certified NERC as the electric reliability organization ("ERO") in its order issued on July 20, 2006 in Docket No. RR06-1-000. *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).
[2] *Supplemental Notice Requesting Comments*, Docket No. RM11-2-000 (February 16, 2011).
[3] *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 this filing may be addressed to:

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook*
Senior 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

Holly A. Hawkins*
Assistant General Counsel
Willie L. Phillips*
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
holly.hawkins@nerc.net
willie.phillips@nerc.net

*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

III. BACKGROUND

On October 6, 2010, the United States National Institute of Standards and Technology ("NIST") identified in a letter to the Commission five foundational families of smart grid standards for consideration.[4] In its letter, NIST stated that it "developed a collaborative process that engages Smart Grid stakeholders in identifying prospective interoperability standards and evaluating these specifications against selected criteria, which include considerations such as stakeholder consensus, domains of applicability, and especially cyber security."[5]

[4] NIST letter to Chairman Jon Wellinghoff (October 6, 2010), available at: http://www.nist.gov/public_affairs/releases/upload/FERC-letter-10-6-2010.pdf.
[5] *Id.*

On January 31, 2011, FERC held a technical conference to discuss whether there was "sufficient consensus"[6] that the proposed NIST smart grid interoperability standards were ready for Commission consideration in a rulemaking proceeding, as directed by section 1305(d) of the Energy Independence and Security Act of 2007 ("EISA"). Section 1305(d) of the EISA provides that:

> At any time after the Institute's work has led to sufficient consensus in the Commission's judgment, the Commission shall institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets.

NIST has formed the Smart Grid Interoperability Panel ("SGIP") to provide an open process for stakeholders to participate in the development of smart grid standards. Although the SGIP does not write standards, it serves as a forum to identify applicable standards, gaps in currently available standards, and priorities for new standardization activities for the evolving smart grid.

As an initial matter, NERC notes that the framework for reviewing smart grid standards used by the SGIP could be improved to achieve greater transparency. At a high level, NERC understands that the first step in the current SGIP process is to identify experts to develop requirement objectives through a Priority Action Plan ("PAP").[7] Then Standards Development Organizations ("SDOs") are selected to create the standard or fill the gap in an existing standard. When the objectives developed by the PAP are completed by the SDOs, the PAP can make a formal request to the SGIP Architecture Committee ("SGAC")[8] and the Cyber Security Working

[6] *See* February Supplemental Notice at P 1.
[7] *PAPs, NIST Smart Grid Collaboration Site*, available at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PriorityActionPlans.
[8] *SGAC, NIST Smart Grid Collaboration Site*, available at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SmartGridArchitectureCommittee.

Group ("CSWG")[9] to review the standards against their interoperability, architecture, and cyber security requirements. However, in its current form, the SGIP sector representatives do not coordinate their responses with sectors they represent. This flaw may result in standards not meeting industry needs.

Both the SGAC and CSWG groups can make recommendations regarding proposed standards. Once the SGAC and CSWG reviews are complete, the PAP can develop a package of standards to be included in the Catalog of Standards ("CoS") and presented to the SGIP Governing Board. The package includes recommendations from individual groups (*e.g.*, CSWG and SGAC) which are prepared through a consensus process. The groups are made up of various stakeholder categories (*e.g.*, vendors, utilities, consultants, academia, and government).[10]

NERC supports efforts by NIST to revise the SGIP process, in coordination with industry stakeholders, so that the framework for reviewing smart grid interoperability standards is clear and transparent to all participants. As part of this enhancement, NERC recommends that SGIP representatives coordinate their responses with the stakeholders they represent.

IV. RESPONSES TO QUESTIONS RAISED IN THE FEBRUARY SUPPLEMENTAL NOTICE

In the February Supplemental Notice, FERC acknowledged that Section 1305(d) of the EISA did not make any smart grid standards mandatory and does not give the Commission authority to make or enforce such standards.[11] Moreover, the Commission noted that under current law, its authority to approve smart grid interoperability standards as mandatory must

[9] *CSWG, NIST Smart Grid Collaboration Site*, available at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG.
[10] Categories of SGIP Membership, available at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCategories.
[11] February Supplemental Notice at P 2 (citing *Smart Grid Policy*, 128 FERC ¶ 61,060 (2009)).

derive from the Federal Power Act ("FPA"). Accordingly, FERC sought comment on questions pertaining to the FERC's authority under the FPA and Section 1305(d).

In formulating its response to the February Supplemental Notice, NERC posted to its website *Directional Topics to FERC's Request for Comment on Smart Grid Interoperability Standards*, seeking input from industry stakeholders, including the Planning, Operating and Critical Infrastructure Protection committee members regarding the content of NERC's response. In that posting, NERC provided reliability considerations and sought input on the three questions discussed below.

- **How does the NIST process assure that a standard has undergone sufficient review of interoperability and cyber security and is ready for consideration by regulators?**

  NERC Response

The development of the smart grid interoperability standards currently coordinated by NIST is directed to enhance communications between devices and equipment rather than the operation of the bulk power system of North America. NERC's Reliability Standards are designed to ensure the reliability of the bulk power system and apply to facilities of the bulk power system. Devices from an array of manufacturers are coordinated to perform multiple control and monitoring functions on generation and transmission to operate the bulk power system of North America. This includes the development of NERC Reliability Standards designed to ensure the protection of cyber assets that are part of the bulk power system.[12] To the extent that the NIST interoperability standards will require designers, vendors, and related

[12] NERC Reliability Standards, available at: http://www.nerc.com/page.php?cid=2|20.

entities to adopt requirements to lessen the risk of cyber penetration, the proposed interoperability standards should be vetted by industry prior to implementation.[13]

The most effective approach to ensure industry support for the final smart grid interoperability standards is to ensure thorough assessments of deployments. This includes experience gained from industry demonstration and testing, including design specification, field deployment, model development and overall assessment of performance.

- **Is it appropriate for reliability and implementation issues to be reviewed by a separate panel, as some panelists commented at the technical conference, composed of utility representatives and NERC?**

  NERC Response

NERC is supportive of reviewing reliability and implementation issues by a separate panel composed of utility representatives and NERC, especially for those issues addressing the management of risk to the reliability, security, and resilience of the bulk power system. As part of the successful integration of smart grid devices and systems, the panel could focus on testing and validation approaches vital to ensure expected benefits are realized, without increased risk to reliability.

- **Whether the criteria for the Commission's evaluation should differ for interoperability and functionality, and the extent to which cyber security is an element of each.**

  NERC Response

As noted above, NERC's primary mission is to ensure the reliability of the bulk power system of North America, and NERC understands the large and increasing role that cyber security occupies in achieving that goal. NERC believes that FERC's evaluation should take

[13] NERC Reliability Standards are developed through an American National Standards Institute accredited process: http://www.nerc.com/docs/standards/sar/Appendix_3A_Standard_Processes_Manual_20100903_2_.pdf.

into account whether the cyber security component impacts the reliable operation of the bulk power system.

A secure critical infrastructure is vitally dependent upon cyber security being engineered in emerging technologies. The legacy paradigm of retrofitting solutions for cyber security should be transformed. Cyber security must be considered at the earliest phases of the smart grid standard development, rather than as an add-on to existing communication protocols.

Cyber security issues are germane both to device functionality and interoperability; however, it is reasonable to expect differing evaluation criteria for each category. Confidentiality, integrity, and availability must be addressed, both for data at rest and data in transit. Remote controls (*e.g.*, automated disconnect) must be tightly secured. Moreover, particular attention must be paid to privacy issues, where disclosure of even the most obfuscated usage patterns could facilitate physical attack. In addition, endpoint controls must be robust to maintain the reliability of the bulk power system.

Cyber security is an element in both interoperability and functionality. For example, data protection through encryption should be specified as an essential function, due to the sensitive and personal nature of individual usage patterns that can be tied to a specific person or household. In order for encryption to work across multiple vendor products and implementations, it must be specified to operate seamlessly between those different implementations, thus, it should be specified for interoperability. Similarly, event records for troubleshooting both operational and security issues should be specified functionally, and should be specified to follow a common format across vendor implementations.

Interoperability for cyber security will be essential for different solutions to be able to interact; therefore, the criteria for approving interoperability standards will be important to the

overall smart grid effort. Cyber security controls that do not seamlessly interoperate will result in wasted resources and will cause confusion by having different incompatible solutions that attempt to solve the same problem. Evaluation for interoperability should focus on the ability of different solutions to operate and communicate with each other in a cyber secure fashion, even if the end result is not the most optimal or efficient solution.

Functionality, on the other hand, does not require the same level of evaluation. Different functional solutions should be accepted, because each functional solution is potentially attempting to resolve a slightly different problem in a different way. Evaluation for functionality should focus on providing solutions that meet real needs, and should focus on whether the proposed solution efficiently and effectively resolves the problem being posed.

The strength of the interoperability design of smart grids, unless carefully planned and operated, can provide a vehicle for intentional cyber attack or unintentional errors impacting bulk power system reliability through a variety of entrance and exit points. Many of the systems implemented using existing smart grid technologies are designed for control functionality and are not responsive to errors resulting from misuse, miscommunications, or information technology system failures. Security of these control systems can be intentionally defeated or unintentionally corrupted by the installation of software updates, for example.

Improvements will be required to provide robust protection from information technology and communication system vulnerabilities. “Defense-in-Depth” approaches, when coupled with risk assessment, can provide an overarching organizational approach to cyber security management. Use of risk assessment can also help determine appropriate defensive measures.

V. CONCLUSION

NERC respectfully requests that the Commission: 1) support NIST efforts to increase the transparency and representation activities of the SGIP process; 2) support industry testing, demonstration, and validation of the NIST smart grid interoperability standards; 3) create a separate panel composed of utility representatives and NERC to address the management of risk to the reliability, security, and resilience of the bulk power system; and 4) investigate the use of "defense-in-depth" and risk assessment to address cyber security implications of smart grid applications, consistent with these comments.

Respectfully submitted,

/s/ Willie L. Phillips

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior 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

Holly A. Hawkins
Assistant General Counsel
Willie L. Phillips
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
holly.hawkins@nerc.net
willie.phillips@nerc.net

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 8th day of April, 2011.

/s/ Willie L. Phillips
Willie L. Phillips
Attorney for North American Electric Reliability Corporation