UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

SMART GRID POLICY) Docket No. PL09-4-000

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO THE COMMISSION'S MARCH 19, 2009 PROPOSED SMART GRID POLICY STATEMENT

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

May 11, 2009

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") is pleased to provide these comments in response to the Federal Energy Regulatory Commission's ("FERC" or the "Commission") March 19, 2009 *Smart Grid Policy, Proposed Policy Statement and Action Plan Order* ("Proposed Policy Statement").[1] NERC applauds FERC's leadership in offering guidance to accelerate the adoption of smart grid technologies and applications, which, as FERC notes, will facilitate the development of common information models for the useful exchange of electric system information, optimize the transmission system to reduce congestion, improve reliability and efficiency of the transmission system, improve energy efficiency, encourage increased awareness of demand response, and support the increased reliance on variable renewable resources.[2]

FERC's stated purpose in its Proposed Policy Statement is to ultimately adopt a policy that will "prioritize the development of key interoperability standards, provide guidance to the electric industry regarding the need for full cybersecurity for Smart Grid projects, and provide an interim rate policy under which jurisdictional public utilities may seek to recover the costs of Smart Grid deployments before relevant standards are adopted through a Commission rulemaking."[3] Because NERC's mission, as the internationally recognized, and FERC-designated Electric Reliability Organization ("ERO"),[4] is to ensure the reliability of the bulk power system in North America by, in part, developing and enforcing mandatory Reliability Standards subject to Commission approval, NERC's comments on this Proposed Policy

[1] *Smart Grid Proposed Policy Statement and Action Plan*, 126 FERC ¶ 61,253 (March 19, 2009), , Docket No. PL09-4-000.
[2] *Id.* at P 12.
[3] *Id.* at P 2.
[4] *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)**.**

Statement focus primarily on the Commission's second stated goal – *i.e.* to determine the Commission's responsibility for approving and enforcing mandatory Reliability Standards for the bulk power system in the United States with respect to smart grid technology and application developments.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:

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

*Persons to be included on the Commission's service list.

III. BACKGROUND

On March 19, 2009, the Commission issued its Proposed Policy Statement providing guidance to support the advancement of a smarter grid for the Nation's electric transmission system.[5] The Commission states in the Proposed Policy Statement that its interest and responsibility in the development of smart grid technologies derives from its authority over the

[5] *See Proposed Policy Statement* at P 1.

rates, terms and conditions of transmission and wholesale sales in interstate commerce.[6] Under the Federal Power Act (FPA), the Commission has jurisdiction over the transmission of electric energy in interstate commerce by public utilities, and over the reliable operation of the bulk-power system the United States.[7] Additionally, the Commission was recently granted the new responsibility of 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" through the Energy Independence and Security Act of 2007 ("EISA").[8] Section 1305(a) of the EISA directs the National Institute of Standards & Technology (the "Institute") "…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."[9]

The Commission refers to "key standards" to be developed with the implementation of smart grid technologies. Based on NERC's review of the Proposed Policy Statement, there are three types of standards (either currently existing or to be developed) that NERC believes will be vitally important to ensuring the successful operation, reliability and security of smart grid technologies. These standards are the three types of standards the Commission refers to in its Proposed Policy Statement – interoperability standards, system security standards and reliability standards.

Interoperability Standards

For purposes of this document, NERC assumes "Interoperability Standards" refer to those standards that provide for: (1) exchanging meaningful, actionable information between two or

---

[6] *Id.* at P 1.
[7] *Id.* at P 5 n.4, *citing to* 16 U.S.C. §§824, 824o.
[8] *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).
[9] *Proposed Policy Statement* at P 7 n.7, citing to EISA §1305(a).

more systems across organizational boundaries; (2) assuring a shared meaning of the exchanged information; (3) achieving an agreed expectation for the response to the information exchanged; and (4) maintaining the requisite quality of service in information exchange (*i.e.* reliability, accuracy, security).[10] The focus of the Commission's Proposed Policy Statement with respect to smart grid devices, networks, and technologies that are able to seamlessly communicate with one another and with system operations centers is on the development of Interoperability Standards.

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. 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.[11] Although there is no cited authority in the Commission's Proposed Policy Statement for the development of System Security Standards, NERC believes it will be important to address these considerations in order to ensure the reliability and security of smart grid systems, networks and technologies.

---

[10] *See Proposed Policy Statement* at n.8, *citing to* GridWise Architecture Council, Interoperability Path Forward Whitepaper at 1-2, 2005, available at http://gridwiseac.org/pdfs/interoperability_path_whitepaper_v1_0.pdf. Footnote 8 of the *Proposed Policy Statement* notes that "[t]he GridWise Architecture Council was formed by the U.S. Department of Energy to promote and enable interoperability among the many entities that interact with the Nation's electric power system." *See* http://www.gridwiseac.org/about/mission.aspx.

[11] *Proposed Policy Statement* at P 30.

Reliability Standards

Reliability standards ("Reliability Standards") are the international standards that ensure Reliability of the bulk power system. Through the Energy Policy Act of 2005,[12] Congress created an ERO, charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. NERC was certified by the Commission as the designated ERO on July 20, 2006.[13] NERC's role as the ERO is to work with the Commission 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.[14] 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 facilities at the transmission and generation level.

With respect to the advancement of smart grid technologies and in response to this Proposed Policy Statement, NERC understands that there could be a need to further advance and develop all three of these types of standards – Interoperability Standards, System Security Standards and Reliability Standards. While NERC understands that the development of Interoperability Standards by the Institute will help implement devices and programs to enable the functionality of a smart grid, NERC's role with respect to this process will specifically be to address whether new Reliability Standards, or modifications to existing mandatory Reliability Standards, will be necessary, to ensure the reliability of the Bulk Power System as new "smart

[12] 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)).
[13] *See North American Electric Reliability Corporation*, 116 FERC ¶61,062 (July 20, 2006)
[14] *See Id.; citing to*, FPA §§ 824, 824o.

grid" technologies are added and interoperability and system security standards are developed to govern their use and deployment.

IV. DISCUSSION

In order to maintain bulk power system reliability and infrastructure protection, planning, and operations will need to evolve with the development of smart grid technologies and applications. While a smarter grid can support bulk power system reliability, new models and tools will be required to design the bulk power system and operate it reliably while incorporating smart grid technologies. Though not insurmountable, these challenges must be studied and technologies developed to ensure that the resulting system achieves greater levels of security and remains reliable.

With the time horizon for transmission system operator decisions measured in cycles and seconds, a smarter grid will enable the wide, seamless, real-time use of applications and tools that provide important information to bulk power system grid operators and managers. For example, in cases of emergencies, grid operators take certain action to recover damaged or compromised sections of the grid, which can be a time-consuming, arduous process requiring significant coordination with field resources as damage is cleared, physical systems and equipment is restored or replaced, and circuits are reconfigured. Restoration from major system disturbances (such as those caused by severe weather) can take days or even weeks to complete the necessary repairs, replacements, and reconfigurations to return the damaged grid to full operation. With the development of a smarter grid, if emphasis is placed, for example, on the role of artificial intelligence to support the human interface in the operations room, such as operator decision support (alerting tools, what-if tools, course-of-action tools), semi-autonomous agent software, visualization tools and systems, performance dashboards, advanced control room design, real-time dynamic simulator training, new data sets, and time-synchronized geographical-based information, these technologies may be more readily available to assist operators in the restoration process, thereby improving safety and restoration times of the bulk power system.

Smart grid technologies at the distribution level also show great promise in supporting the further development of demand-side resources, notably including demand response, price-responsive management of new "behind-the-meter" generation such as rooftop solar panels, and potential new loads such as Plug-In Hybrid Electric Vehicles.

While smart grid implementation will require the development of tools that will enable transmission system operators to take advantage of, for example, the bidirectional flows of communications and energy, this evolving design and operation of smart grid technologies must be built and implemented while ensuring the reliability and security of the bulk power system. Accordingly, NERC plans to work in close collaboration with other existing standards-setting bodies and with the Commission to ensure that reliability and security of the bulk power system is maintained.

A. Standards Development

In its Proposed Policy Statement, the Commission, in addressing the adoption of smart grid standards, provides that the Institute "will recommend standards to the Commission that have resulted from the Institute's coordination with standards development organizations and technical experts."[15] The Commission provides that once "sufficient consensus" on interoperability standards has been achieved, the Commission will institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to ensure smart grid functionality and interoperability in the interstate transmission of electric power, and regional

[15] *Proposed Policy Statement* at P 9.

and wholesale electricity markets.[16] The Commission states that it expects the Institute will recommend to the Commission, in accordance with Section 1305(a) of the EISA, interoperability standards that have been developed in coordination with standards development organizations and industry participants, which will result in the development and implementation of a smart grid.[17]

NERC, like IEEE (formerly known as the Institute of Electrical and Electronic Engineers), the National Electric Manufacturers Association ("NEMA"), and the North American Energy Standards Board ("NAESB"), is one of several American National Standards Institute ("ANSI") accredited standards-setting bodies. NERC is responsible for developing Reliability Standards for the reliability and security of the bulk power system. Given NERC's position as a standards-setting organization, NERC believes the Institute's development of Interoperability Standards must work in coordination with existing Reliability Standards and other standards-setting bodies. In particular, without adequate coordination among Interoperability Standards, System Security Standards, and Reliability Standards, the high level of detail required for smart grid interoperability needed to maintain bulk power system reliability and security may not be achieved. In fact, reliability of the bulk power system is paramount for smart grid technology to be effective because in all cases, if reliability is not maintained, interoperability of smart grid technologies will either become less valuable or inoperable due to reliability issues. Therefore, maintaining a reliable bulk power system is essential to the successful application and implementation of smart grid technologies.

Experience with standards development in the communications and information technology industries has shown that the development of such standards requires the full

[16] *Id.* at P 8 n.9, citing to EISA §1305(d).
[17] *Proposed Policy Statement* at P 9.

involvement of many industry participants. However, even with this level of involvement, products built or operated in accordance with the resulting standard may be fully compliant with the standard itself, but not interoperate effectively. Additionally, many interoperability standards required for smart grid technologies and applications will be developed outside of the electric industry (*e.g.*, advanced telecommunications and information transfer), over which FERC will not have jurisdiction. Accordingly, NERC will actively support FERC in working with the Institute and the industry to articulate clear policy guidance for the development of smart grid technologies and applications, including the development of Interoperability Standards, in such a way that recognizes the reliability of the bulk power system.

With respect to the Commission's statement that it intends, in order to fully incorporate measures to protect against cyber and physical security threats, to advise the Institute to take the necessary steps to assure that its process for the development of any interoperability standards and protocols leaves no gaps in cyber or physical security unfilled,[18] NERC supports the proposed request from FERC to the Institute and the industry to develop secure Interoperability Standards that address these issues. NERC believes there is a shared responsibility, from supplier to user, to address cyber security. Designing security into devices and architectures from the outset will provide for greater protection and will be more cost effective than if this security were to be added after the equipment is built and deployed. NERC also believes that even with secure, smart endpoint devices, without an additional layer of interoperability issues being addressed, there are simply too many ways that the security of smart grid devices could be compromised.

Accordingly, NERC supports the Commission's identification of security (cyber and physical) and a common semantic framework for grid information exchange in smart grid

[18] *Id.* at P 15.

standards development, and will work collaboratively with FERC and other standards-setting organizations in addressing these concerns through the various standards-setting development processes.

B. Urgency of Achieving Certain Smart Grid Functionalities

In its discussion regarding the urgency of achieving certain smart grid functionalities,[19] the Commission notes its particular interest in the development of smart grid functions and characteristics that can help address challenges to the Commission-jurisdictional bulk power system.[20] NERC, as the designated ERO responsible for developing and enforcing mandatory Reliability Standards with respect to the bulk power system subject to Commission approval, looks forward to working with the Institute in developing standards that will help advance the development of smart grid technologies, and addresses specific areas in which NERC mandatory Reliability Standards could be required to be modified or developed.

1. Cyber Security and Reliability

The Commission notes in its Proposed Policy Statement, that the purpose of the ultimately adopted Smart Grid Policy Statement is, among other things, to "provide guidance to the electric industry regarding the need for full cybersecurity for Smart Grid projects,"[21] and "to make consistency with cybersecurity and reliability standards a precondition of its adoption of Smart Grid standards."[22] NERC fully agrees that cyber security for smart grid technologies should be a top priority. NERC further agrees that close coordination will be required with the Institute as jurisdictional overlaps could potentially occur.

---

[19] *Id.* at PP 11-12.
[20] *Id.* at P 12.
[21] *Id.* at P 2.
[22] *Id.* at P 14.

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 FPA, 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. However, the possible aggregated impacts of these smart grid devices to the security of bulk power system with the addition of thousands or millions of smart grid devices can be substantial.

For example, 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 their control.

Furthermore, while the majority of reliability risks to the bulk power system result in probabilistic failures that can be studied and accounted for in planning and operating assumptions, cyber risks will likely require an alternative approach. As such, the industry should not rely on studies of real world events to learn protection priorities. Instead, the industry should apply the concept of simultaneous loss of assets or common modal failure in scale to determine how we can identify what needs to be protected. Therefore, NERC intends to closely follow the Institute's development of Standards for these smart grid technologies and their associated network and system architectures, and collaboratively work with the Institute to develop these standards with an eye towards aggregated impacts to the bulk power system. NERC encourages FERC to adopt policies that encourage the Institute to use its role, as the smart grid standards proponent and coordinator, to build cybersecurity protections into standards that affect the full span of smart grid players, such as the distribution system, utilities' business systems, customer appliances, and IT systems.

2. Inter-system Communication and Coordination

In its Proposed Policy Statement, the Commission notes that "[t]here is an urgent need to further develop a common semantic framework (i.e., agreement as to meaning) and software models for enabling effective communication and coordination across inter-system interfaces."[23] The Commission specifically provides that in order to enable a smarter grid, particularly one capable of addressing bulk power system challenges, effective interfaces must be developed between and among all of these systems.[24] NERC agrees, and supports the Commission's proposal that the development of inter-system interfaces should be a high priority for accelerated development because, for example, new and legacy control systems will need to be able to communicate with each other. Adoption of smart grid standards to address this need could play an important role in the movement to a smarter grid, which would be capable of addressing challenges to the reliability and security of the bulk power system. NERC therefore supports the Commission's efforts in developing smart grid technologies and independent control systems that will be capable of communicating with existing bulk power control systems (*e.g.* load-

---

[23] *Id.* at P 16.
[24] *Id.* at P 16.

generation balancing systems), and believes this effort is crucial to maintain reliability of the bulk power system.

3. Integrating Renewable Resources into the Electric Grid

With respect to integrating renewable resources into the electric grid, FERC points out that as of December 2008, the Nation had 25,170 MW of wind generation based on nameplate capacity,[25] and according to NERC's 2008 Long-Term Reliability Assessment, an additional 145,000 MW of wind power projects are planned or proposed over the next ten years.[26] NERC agrees with FERC that the functionalities of smart grid technologies and applications can potentially provide the flexibility necessary to reliably integrate large amounts of variable generation.[27]

C. Development of Key Interoperability Standards

In its Proposed Policy Statement, the Commission notes that with a strong national interest in expediting the development and deployment of the types of technologies and capabilities associated with a smarter grid, there is also a need to prioritize the development of two cross cutting issues that comprise the first level of work to be accomplished in the interoperability standards-setting process.[28] These two crossing cutting issues are system security (*i.e.*, cybersecurity and physical security to protect equipment that can give access to smart grid operations), and communications (*i.e.*, a common semantic framework and software models for enabling effective communication and coordination at the boundaries of utility systems where these interface with customer and other systems, thereby providing "inter-system"

---

[25] *Id.* at P 18.
[26] NERC 2008 Long-Term Reliability Assessment, 2008-2017, p. 9, 12, October 2008, available at http://www.nerc.com/files/LTRA2008v1_2.pdf
[27] *See* NERC Special Report, *Accommodating High Levels of Variable Generation*, available at http://www.nerc.com/files/IVGTF_Report_041609.pdf
[28] *Proposed Policy Statement* at P 25.

functionality).[29] FERC then associates four priority grid functionalities (wide-area situational awareness, demand response, electric storage, and electric transportation) with these cross-cutting issues.[30] While NERC's focus with respect to the development of smart grid technologies is on the development of Reliability Standards, NERC provides comments on the Commission's two overarching principles – System Security and Communications – in order to explain how the development of smart grid technologies in these two areas could specifically impact reliability of the bulk power system. NERC then addresses the four priority grid functionalities (wide-area situational awareness, demand response, electric storage, and electric transportation) and their potential impact on the bulk power system.

1. Two Overarching Principles – System Security and Communication

With respect to system security, the Commission notes that a "responsible entity subject to Commission-approved reliability standards, such as the CIP Reliability Standards, must ensure that it maintains compliance with those standards during and after the installation of smart grid technologies.[31] Indeed, NERC agrees with the Commission that compliance with existing CIP Standards during and after the installation of smart grid technologies is important. However, NERC believes it will also be critical to develop new CIP Reliability Standards, as necessary, and ensure compliance with existing CIP Reliability Standards in order to maintain reliability of the bulk power system with the development of smart grid technologies. As technological advancements change the way we do business, there may be a need to re-evaluate those systems that need to be protected and determine how best to achieve appropriate levels of security. For example, in the future, there may be a need to shift from a focus on cyber assets that support physical assets to a focus on data that supports critical functions or decisions.

[29] *Id.* at P 28.
[30] *Id.* at P 28.
[31] *Id.* at P 29.

Additionally, the Commission provides for interoperability and cyber controls, which NERC refers to as System Security Standards.[32] While these standards could help to ensure reliability by requiring a common framework for the development of smart grid system architectures and technologies, the system architectures and technologies that will make up a smarter grid must be evaluated to determine whether they are Critical Assets, subject to NERC's CIP Reliability Standards.[33] The NERC CIP Standards, without special directed application, would normally not be applied by utilities to address smart grid related technologies and architectures in the distribution realm, for example. Therefore, additional security requirements may be necessary, so that devices, protocols, and network designs can be operated in a way that adequately supports the integrity of the technology and its applicability to a smarter grid while operating in such a way that enables reliability of the bulk power system.

Additional development of CIP Reliability Standards resulting from smart grid technologies will enable a safe and reliable bulk power system. Therefore, NERC will follow the Institute's efforts in developing Interoperability Standards and the development of System Security Standards closely to determine whether any changes are necessary to NERC CIP Reliability Standards in order to maintain bulk power system reliability.

[32] *Id.* at P 30. These controls include (1) the integrity of data communication (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 or person); (3) the prevention of unauthorized modifications to Smart Grid devices and the logging of all modifications made; (4) the physical protection of Smart Grid devices; and (5) the potential impact of unauthorized use of these Smart Grid devices on the bulk-power system.

[33] NERC Reliability Standard CIP-002-1, Requirement 1, requires the responsible entity to "identify and document a risk-based assessment methodology to use to identify its Critical Assets." NERC is currently in the process of drafting a guideline on how to identify Critical Assets that is out to stakeholders for comments. Nonetheless, identification of Critical Assets will be important in the development of smart grid technologies.

2. Four Priority Grid Functionalities

i. Wide-Area Situational Awareness

NERC appreciates FERC's recognition of the value of wide-area situational awareness as a critical, high-priority in smart grid technologies and applications. Wide-area situational awareness is critical for maintaining a high level of bulk power system reliability and preventing or mitigating disturbances. Visualization is one of several means for delivering wide-area situational awareness to operators, along with alarms, messaging, and automated device actions and options analysis.

NERC's work with utility industry leaders, the Department of Energy, National Labs and the vendor and consulting communities through the North American SynchroPhasor Initiative ("NASPI") is helping to accelerate the value of synchrophasor technology across the bulk power system. Regional transmission organizations ("RTOs") have been active in NASPI and will play increasingly important roles in its implementation to protect bulk power system reliability. But because RTOs and Independent System Operators ("ISOs") do not own physical transmission assets, they must work with transmission owners, generation owners and balancing authorities to install needed phasor-related technology in the field, including phasor measurement units ("PMUs"), phasor data concentrators, and communications links. Therefore, while RTOs can help to lead and coordinate, they cannot bear the full responsibility for synchrophasor technology application.

NERC's work with NASPI through its development of the NASPInet is one example of a system that will further promote and assist in the development of wide-area situational awareness, namely the SynchroPhasor Initiative. The NASPInet architecture design for a NASPI data communications system is a research project funded by the U.S. Department of Energy, with the cooperation and support of NASPI community experts. It will require further development, testing and pilot applications (coordinated by DOE, NASPI and the electricity, information technology, and communications industries) before the NASPInet design (or its successor) is ready to be adopted into a formal standard for industry use. There may also be value in applying the underlying communications systems (on which NASPInet is implemented) into a widely applied smart grid backbone communications system that links bulk power assets. Such issues should be fully explored before an early-stage concept such as NASPInet is accepted as a formal standard.

Additionally, because the number of PMUs has been growing slowly over the past five years, and the volume and quality of phasor data on grid conditions has been changing, we do not yet have a definitive understanding of what real-time phasor data can tell us about present and near-term grid conditions. It may take several years of research before such understanding is fully achieved.

In its Proposed Policy Statement, FERC notes that increased deployment of PMUs can enable more efficient use of the grid, for example through a switch from static to dynamic line ratings.[34] While this may be correct, NERC's primary interest in accelerating the use of synchrophasor technologies is to improve and protect bulk power system reliability. Although phasor data and applications will eventually enable better use of grid assets for market purposes (*i.e.* congestion reduction), the highest value and best-supported early synchrophasor applications are for reliability.

The Commission's Proposed Policy Order also notes the challenges of developing software and systems for managing, processing and delivering large volumes of phasor data into forms useful for operators and control systems, and suggests that the Institute should identify the

[34] *Id.* at P 36.

core requirements for such software and systems.[35] NERC believes that such efforts have been underway for several years under the guidance of DOE's Visualization and Controls R&D program and the work of several utilities, including Tennessee Valley Authority ("TVA"), Bonneville Power Administration ("BPA") and the California ISO ("CAISO"), that have focused aggressively on these issues. Given that such entities must design, implement and use these grid-critical software and hardware systems, and integrate them with other applications and functions, NERC believes that they should remain the responsible entities guiding core requirements, and that the Institute should not assume responsibility for this effort.

ii. Demand Response

With respect to Demand Response, NERC notes that smart grid technologies and applications can enable enhanced application of demand response resources for wide-area applications, including the integration of variable resources. Specifically, demand response can enable the enhanced communication and real-time coordination of information between system operators and customers; can provide greater confidence and operational flexibility that can provide increased access to ancillary services and supporting variable generation; can provide direct control or optimization of "smart devices and/or appliances" with automated signals that can respond to system events, conditions, or contingencies; can support distributed storage capabilities to provide system regulation support; and can provide capacity reserves (spin and non-spin) coupled with Automatic Generation Control ("AGC") or Area Control Error ("ACE") types of technologies.[36]

---

[35] *Id.* at P 36.
[36] ***See*** Special Report, *Accommodating High Levels of Variable Generation*.

Demand Response penetration is on the rise, contributing more and more to supply portfolios.[37] Therefore, the measurement and verification of these resources must be transparent, complete, and accurate. To date, with respect to Demand Response, NERC is collaboratively working with the North American Energy Standards Board ("NAESB") to develop both retail and wholesale demand response measurement and verification standards on definitions of demand response resources, and is developing a NERC Demand Response Availability Data System ("DADS") system that will support the tracking of historical performance data for Demand Response.

However, reliability implications could arise with respect to Demand Response. For example, smart meters are being designed that will communicate prices to consumers, and some meters will have the ability to directly control consumer appliances. While planners and operators of the bulk power system currently plan and operate their systems based upon load diversity resulting from uncontrolled electric use by consumers, smart meters may remove some of that diversity. If not properly planned, removing some of this diversity could result in unintended consequences.

Therefore, NERC requests that the Commission consider these types of issues that could arise during thee implementation of Demand Response programs. NERC will continue to study this issue through its Integrating Variable Generation Task Force ("IVGTF") working group, and will work collaboratively with FERC and other standards-setting bodies to ensure that reliability implications resulting from the increased use of Demand Response are addressed.

iii. Electric Storage

FERC recognizes in its Proposed Policy Statement that "[if] electricity storage technologies could be more widely deployed, they would present another important means of

[37] *See* NERC's 2008 Long-Term Reliability Assessment at p 18.

addressing some of the difficult issues facing the electric industry."[38] NERC agrees with the Commission's statement and has recently actively been addressing the issue of energy storage through the stakeholder process to determine how the integration of energy storage affects reliability of the bulk electric system.

To date, NERC's IVGTF has identified the issue of energy storage, and plans to address it further in the next phase of its work plan. Specifically, the IVGTF will assess the influence on bulk power system reliability of accommodating large amounts of charging and discharging electric vehicles, storage and demand response associated with smart grid technologies and advancements, including integration on the distribution system.[39] Additionally, the IVGTF will "[s]tudy the impact of distributed variable generation on bulk power system reliability."[40] NERC believes it is important that the industry undertake more research and development in order to develop lower cost, reliable and safe electric storage.

Going forward, NERC recommends that FERC adopt standards and protocols on electric storage that the Institute determines are appropriate after achieving significant consensus investigating storage applications. Additionally, NERC plans to work collaboratively with the Commission and the Institute on electric storage issues that could have an impact on bulk power system reliability.

iv. Electric Transportation

FERC provides in its Proposed Policy Statement that another key grid functionality, electric transportation, must be addressed with respect to its level of influence on the reliability of the bulk power system and how and when electric transportation draws electricity off of the

---

[38] *Proposed Policy Statement* at P 40.
[39] *See* Special Report, *Accommodating High Levels of Variable Generation*.
[40] *Id* at p 71.

bulk power system.[41] While NERC agrees with FERC that development of electric transportation is an important area for smart grid advancements, not only to enable the development of plug-in hybrid electric vehicles ("PHEV's"), but also to reliably integrate them into the grid, there are currently few PHEVs or electric vehicles ("EV") in use. Therefore much of the work to date with respect to electric transportation has been based on forecasting and theoretical assumptions. While there are currently relatively small numbers of PHEVs and EVs in North America, the earliest projections for mass production are for 2010. The current grid infrastructure has not been developed to optimally integrate PHEVs (*i.e.* price-signaling, off-peak charging automation). Upgrades (generally at the distribution level) may be necessary in the near-term, but the infrastructure impact will depend on the PHEVs themselves. Additionally, the current grid was engineered for one-way energy distribution flow, not two-way flow of power, so the grid is not optimized for vehicle-to-grid power flow.

Therefore, the reliability of the bulk power system could be impacted by high levels of the penetration of PHEVs because charging at consumer convenient times (late afternoon after work, for example) will increase peak demand and could create the need for more generation or transmission. Additionally, while individual PHEV's will not directly connect to the bulk power system, a high penetration of PHEV's could provide sufficient load or distributed power storage to support bulk power reliability. Accordingly, the complexity of managing demand and energy could change dramatically.

While NERC, in coordination with the IVGTF, has addressed this issue and plans to review it further in the next phase of its work plan, NERC recognizes that with the addition of increased amounts of PHEVs and EVs and their potential impact on the bulk power system, NERC Reliability Standards may have to be modified to take these considerations into account.

[41] *Proposed Policy Statement* at P 41.

NERC will work closely with the Commission and standards-setting bodies on these types of issues to ensure that reliability and security of the bulk power system is maintained.

V. <u>CONCLUSION</u>

NERC is pleased to provide these comments in anticipation of the Commission's issuance of a Policy Statement to further develop policies and procedures for the advancement and development of smart grid technologies. However, for the reasons stated above, NERC urges the Commission and standards-setting bodies that will participate in the development of smart grid technologies to ensure that the bulk power system remains safe and reliable throughout all phases of development and implementation of a smarter grid.

Therefore, NERC encourages FERC to consider in its final policy statement the need for development of Interoperability Standards and System Security Standards that work collaboratively and in conjunction with NERC mandatory Reliability Standards. Because cybersecurity and reliability will be of paramount importance in the development of a smarter grid, NERC urges the Commission to develop policies relating to smart grid technologies that ensure the safety and reliable operation of the bulk power system. Ultimately, without a safe and reliable grid, smart grid technologies, no matter how technologically advanced, will not operate effectively.

Respectfully submitted,

<u>/s/ Rebecca J. Michael</u>

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

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

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 11th day of May, 2009.

/s/ Holly A. Hawkins
Holly A. Hawkins

Attorney for North American Electric Reliability Corporation