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 (DRAFT NISTIR 7628)

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
michael.assante@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

December 1, 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") Smart Grid Cyber Security Strategy and Requirements Draft document ("Smart Grid Cyber Security 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 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 Smart Grid Cyber Security Document 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, September 2009 ("Smart Grid Cyber Security 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
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
michael.assante@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 Smart Grid Cyber Security Document was developed by the Smart Grid Cyber Security Coordination Task Group ("CSCTG") to describe the overall cyber security strategy for the Smart Grid. NIST states that the "[i]mplementation of a cyber security strategy requires the development of an overall cyber security risk management framework for the Smart Grid," and defines risk as "the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts."[3] The primary focus of NIST's proposed cyber security strategy appears to be on the information technology ("IT") and telecommunications infrastructures and how those areas interact with energy sector infrastructure. For example, the Smart Grid Cyber Security Document states that "[w]ith the Smart Grid's transformation of the electric system to a two-way flow of electricity and

[3] Smart Grid Cyber Security Document at p. 3.

information, the [IT] and telecommunications infrastructures have become critical to the energy sector infrastructure," and "the management and protection of systems and components of these infrastructures must also be addressed by an increasingly diverse energy sector."[4] NIST notes that the "goal is to ensure that a comprehensive assessment of the systems and components of the Smart Grid is completed," and that "the next step is to select and tailor (as necessary) the security requirements."[5] The Smart Grid Cyber Security Document is NIST's preliminary report describing the overall cyber security strategy for the Smart Grid.

On March 19, 2009, FERC issued a document entitled *Smart Grid Policy, Proposed Policy Statement and Action Plan Order* ("Proposed Policy Statement")[6] on which NERC provided comments. The Commission issued a Final Policy Statement on July 16, 2009,[7] 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,"[8] NIST, in accordance with the Energy Independence and Security Act of 2007 ("EISA"), Section 1305(a), was directed "to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth." NIST was also tasked with the responsibility of coordinating "the development of a framework that includes protocols and

[4] *Id.* at p. 1.
[5] *Id.* at p. 3.
[6] *Smart Grid Policy*, "Proposed Policy Statement and Action Plan," 126 FERC ¶ 61,253 (March 19, 2009), Docket No. PL09-4-000 ("FERC Proposed Policy Statement").
[7] *Smart Grid Policy*, "Policy Statement," 128 FERC ¶ 61,060 (July 16, 2009), Docket No. PL09-4-000 ("FERC Policy Statement").
[8] 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).

model standards for information management to achieve interoperability of smart grid devices and systems."[9]

NERC also provided comments to NIST in response to the NIST Framework and Roadmap for Smart Grid Interoperability Standards document[10] on November 9, 2009.[11] NERC's comments on that document specifically focused on the development of voluntarily Interoperability Standards as they relate to NERC's mandatory Reliability Standards, and in particular, to NERC CIP Reliability Standards.

Based on NERC's review of the NIST Smart Grid Framework Document and the Smart Grid Cyber Security Document, there are three types of standards (either currently existing or to be developed) 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 Smart Grid 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 responses. The reliability, fidelity, and security of information exchanges between and among Smart Grid systems must achieve requisite performance

[9] FERC Proposed Policy Statement at P 7 n.7, citing to EISA §1305(a).
[10] *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").
[11] 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.

levels."[12] "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 and interoperability. They define specifications for languages, communication 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."[13]

NERC notes that the Interoperability Standards proposed in the Smart Grid Framework Document and the Smart Grid Cyber Security Document appear to focus on components and applications, and in many cases do not directly address interoperability of networks and systems and do not adequately protect against potential cyber security vulnerabilities that could penetrate the Smart Grid. That is, the proposed Interoperability Standards are useful today for component designers and manufacturers, but may not be adequate for system integrators and the electric power industry to guide architectures and system properties and prevent potential cyber security attacks. 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

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

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.[14] Although there is no cited authority in the Smart Grid Cyber Security Document, NERC believes it will be essential in addressing cyber security considerations to ensure that standards for the design and integration of Smart Grid systems, networks and technologies do not conflict with or create unintended reliability and security risks for the bulk power system.

NERC Reliability Standards

NERC Reliability Standards ("Reliability Standards") are the international standards that ensure reliability of the North American bulk power system. Through the Energy Policy Act of 2005,[15] 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[16] and is similarly recognized by applicable governmental authorities in Canada. NERC's role as the ERO is to develop, implement, and enforce mandatory Reliability Standards for the bulk power system, in the United States subject to Commission approval, in accordance with Section 215 of the Federal Power Act (the "Act" or the "FPA").[17] 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

[14] FERC Proposed Policy Statement at P 30.
[15] 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)).
[16] *See* North American Electric Reliability Corporation, 116 FERC ¶61,062 (July 20, 2006).
[17] *See Id.*; citing to, FPA §§ 824, 824o.

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 an overall cyber security strategy for the Smart Grid and its development of Interoperability Standards will help to implement devices and programs that enable the functionality of a Smart Grid, NERC's role with respect to this process is to specifically address whether new Reliability Standards, or 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. Additionally, given NERC's responsibility in ensuring adequate cyber security of the bulk power system, NERC is specifically focusing these comments on potential cyber security vulnerabilities that it encourages NIST to consider in its development of an overall cyber security strategy for the Smart Grid.

IV. DISCUSSION

The Smart Grid Cyber Security Document describes NIST's overall cyber security strategy for the Smart Grid by analyzing use cases, requirements and vulnerability classes identified in other cyber security assessments and scoping documents, and other information necessary for specifying and tailoring security requirements to provide adequate protection for the Smart Grid.[18] NIST states that ultimately, the Smart Grid Cyber Security Coordination Task Force will develop a comprehensive set of cyber security requirements.[19] The Smart Grid Cyber

[18] *See* Smart Grid Cyber Security Document at p. 1.
[19] *Id.* at p. 1.

Security Document is the first step in the development of a set of cyber security requirements applicable to the Smart Grid. NERC's comments herein focus on suggested areas for NIST's further consideration in the development of a cyber security strategy for the Smart Grid, and how the overall cyber security strategy should influence the development of a set of cyber security requirements. As discussed below, there are very important cyber security considerations that will impact the Smart Grid that NERC believes must be included in NIST's overall cyber security strategy.

As a general matter, NIST discusses the importance of interfaces in the Smart Grid Cyber Security Document and explains how these interfaces will come together to create the Smart Grid. NERC agrees that these interfaces are important, and recommends that Interoperability and System Security 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. While the focus in the Smart Grid Cyber Security Document is on devices, developing a better communications gateway or smart meters will not ensure the integrated devices will provide sufficient cyber security of the Smart Grid. Issues will arise in the integration of these systems that will require attention.

One method NERC recommends for NIST's consideration in the development of an overall cyber security strategy of the Smart Grid is to develop standards that apply to the integration of these systems required for use by their integrators. NERC discusses these concepts in more detail below in its discussion of specific sections of the Smart Grid Cyber Security Document.

Comments on Specific Sections of the Smart Grid Cyber Security Document

1. Section 1.2: The Energy Independence and Security Act Requires that Standards be Developed to Maintain a Reliable and Secure Electricity Infrastructure That Can Meet Future Demand and Growth.

In Section 1.2 of the Smart Grid Cyber Security Comments, NIST states that, in accordance with the Energy Independence and Security Act of 2007, the U.S. will support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth.[20] There are two objectives that NIST states will be important in achieving a Smart Grid. These are:

1. [The] [i]ncreased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid; and

2. Dynamic optimization of grid operations and resources, with full cyber-security …[21]

While NERC agrees these two categories are important areas in achieving a Smart Grid, NERC notes that there is no such thing as full cybersecurity. That is, there is no "cyber security model" that, once achieved, will ensure full protection of the Smart Grid. There currently is no cyber security model that will accomplish complete security of the Smart Grid. Therefore, it is important that NIST understand that there are different levels of maturity involving the Smart Grid, and integration of new parts and pieces into the Smart Grid could present cyber risks because there is no industry-accepted cyber security strategy.

NERC proposes two strategies in 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

[20] *Id.* at p. 2.
[21] *Id.*, citing to EISA of 2007, P.L. 110-140.

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, thereby 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.

2. Section 1.3: NIST's Discussion Regarding Overall Risk to the Electric System Should be More Inclusive Because the Smart Grid Will Affect the Electric System from Generation to Meter.

In Section 1.3 of the Smart Grid Cyber Security Document, NIST states that "[c]yber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters."[22] NIST continues that "[v]ulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways."[23] Given the seriousness of potential cyber security vulnerabilities on the Smart Grid, NERC believes it is critically important that NIST's assessment of an overall cyber security strategy for the Smart Grid be more inclusive than what is presented in the Smart Grid Cyber Security Document because it will affect the operation of the electric system from generation to meter.

One suggestion NIST should consider is to expand its risk assessment to address three components: distribution, transmission and generation. The Smart Grid will equally create risk

[22] *Id.* at p. 2.
[23] *Id.*

across all three of these functions. Additionally, there will be an increased potential for attacks, not only in those areas where electrons flow for power, but also where communications take place. With the Smart Grid, significant technology additions will be made in the distribution environment, thereby introducing the possibility of cyber security attacks on the distribution system.

In Section 1.3 of the Smart Grid Cyber Security Document, NIST states that, "[w]ith the adoption and implementation of the Smart Grid, the IT and telecommunications sectors will be more directly involved," and it therefore proposes that IT and telecommunications cyber vulnerabilities for these areas be assessed in the context of Smart Grid.[24] While NERC agrees that the introduction of new IT and telecommunications equipment will introduce tools to the Smart Grid that are more mature than some current industrial control applications, having the ability to protect these new applications (*i.e.* IT and telecommunications) from cyber security risk will not guarantee that the Smart Grid as a whole is protected from a potential cyber attack.

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. 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

[24] *Id.*

will be integrated to make up the Smart Grid, thereby potentially introducing new cyber security vulnerabilities on a regular basis.

NIST concludes Section 1.3 by defining cyber security as the "protection required to ensure confidentiality, integrity and availability of the electronic information communication system."[25] While this definition focuses on the information communications system in cyber security of the Smart Grid, it is not a broad enough definition to ensure adequate cyber security of the Smart Grid. Rather, it leaves the impression that the lack of cyber security or the impact of cyber security vulnerabilities are confined only to the information communication systems of the Smart Grid. This is not the case. Potential cyber security vulnerabilities could apply to all areas of the Smart Grid, including the performance of physical equipment. That is, cyber security implications can materially impact the industry's ability to provide commands that actually transpose the boundary from a cyber command communication to a Remote Terminal Unit ("RTU") specifying an operating voltage to a device that results in a physical action (*i.e.* the opening or closing of a switch). Therefore, NIST's definition for cyber security must include more than just those elements that are linked to the information and communication systems.

3. Section 1.4.2: There is a Continuous Risk Assessment Associated with the Smart Grid; That is, Every Time a New Piece or Part is Integrated, New System Vulnerabilities are Introduced. Therefore, a Common Lexicon or Language Should be Developed that Will Help the Industry to Better Understand How to Manage Risk.

In Section 1.4.2, NIST explains its risk assessment of the Smart Grid by identifying potential vulnerabilities and describing how it examined the impacts and threats to the Smart Grid from both a high-level overall functional perspective as well as a focus on the six functional

[25] *Id.* at p. 3.

priority areas that are the focus of the Smart Grid cyber security strategy.[26] NIST explains that the output will be used in the selection of security requirements and identification of security requirement gaps.[27] Based on its risk assessment, NIST proposes an overall cyber security strategy for the Smart Grid, including proposed cyber security standards that should be included in the body of Interoperability Standards.

NIST's overall risk assessment is flawed because it does not capture the essential idea that Smart Grid is not a point in time. That is, one specific action cannot be taken regarding cyber security that will protect the system as a whole. Because the Smart Grid will evolve in pieces and parts, every time a new piece or part is integrated into the Smart Grid, new system vulnerabilities and variations on consequences could be introduced. Very rarely will the introduction of a new piece or part take vulnerabilities away. Therefore, when they are integrated into the Smart Grid, that piece or part must be customized to ensure that cyber security is integrated into system architectures. Additionally, there must be a continuous focus on cyber security protection of equipment that is integrated into the Smart Grid from a bulk power system planning design and operation perspective. Anytime a new piece or part is introduced, an assessment of potential cyber security vulnerabilities and consequences if successfully exploited is required so the industry can adequately protect that equipment from a potential harm. This process must be well-defined, continuous with the growth of the Smart Grid, and coordinated amongst the industry.

[26] *Id.* at p. 5. The six functional areas, which are identified in the Smart Grid Framework Document at p. 6, are: demand response and consumer energy efficiency; wide area situational awareness; electric storage; electric transportation; advanced metering infrastructure; and distribution grid management. There are an additional two areas for consideration that were presented in the Smart Grid Framework Document. These two areas are: cyber security and network communications.

[27] *Id.*

One approach that NIST should consider in ensuring that the process of continually assessing cyber security risks to the Smart Grid is performed is to develop a common lexicon or language to capture system or function vulnerabilities that require continual monitoring of cyber security weaknesses. This common lexicon could be modeled after the Mitre Common Weakness Enumeration ("CWE")[28] or a similar, common enumeration. The CWE provides a common language of discourse for discussing, finding, and dealing with the causes of software security as they are found in code, design, or system architecture.[29] A similar lexicon could be developed to enable the discussion of cyber security vulnerabilities, particularly for those potential cyber security vulnerabilities and risks of the Smart Grid. This common lexicon will also help to enable the secure planning, design and operation of the bulk power system.

For example, today NERC might receive a message from a Reliability Coordinator regarding its SCADA system indicating that it "lost visibility." However, because there are no agreed-upon definitions, industry stakeholders may not necessarily know the context or ramification for this statement. Therefore, the development of a common lexicon will support the industry in understanding what is meant by providing a clearer understanding of what actions are needed to protect the security of the electric grid.

Additionally, because the Smart Grid will be developed in components, pieces, or systems, each one should have its own method of communicating to the system its operational status. With these methods of communication, each system's operational status could be communicated in such a way that a system operator will immediately know whether a system is vulnerable to cyber security attacks and therefore, what the vulnerabilities are and if the components, pieces or systems should be interconnected. A system's operational status could be

[28] *See* http://nvd.nist.gov/cwe.cfm for more information on MITRE's Common Weakness Enumeration.
[29] *See id.*

categorized in three categories: (1) a "fully capable" system is a system that is capable of doing all of the things that is needs to do and is believed to be cyber-secure; (2) a "degraded" system is a system that can only do certain things without cyber risk; and (3) a "not capable" system is a system that is not capable of performing its primary mission, and as such, requires that it be taken out of operation.

These three categories describing operational status of systems are one method of providing the industry with the tools it needs to understand what the problems are with respect to cyber security risk for the systems that will make up the Smart Grid. These considerations should be considered in the planning side too. Ultimately, a common lexicon to assess cyber security risk, along with a method of assessing a system's operational status, will provide a better view to the industry of potential cyber security vulnerabilities and what losses to a system mean for the reliability and security of the electric grid.

4. Section 1.4.4: NIST States that the NERC CIP Standards are Mandatory for a Specific Domain of the Smart Grid. This is not accurate. NERC's Reliability Standards Only Apply to Users, Owners, and Operators of the Bulk Power System.

In Section 1.4.4 of the Smart Grid Cyber Security Document, NIST states that currently only NERC CIP Reliability Standards are mandatory for a specific domain of the Smart Grid. In fact, NERC's Reliability Standards not only apply to a specific domain of the Smart Grid, they also only apply to specific parties. 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. Therefore, caution should be used in applying NERC CIP Reliability Standards to an overall cyber security strategy for the Smart Grid 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. However, 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. Therefore, 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 overall cyber security strategy for the Smart Grid will not, by themselves, adequately protect cyber security of all components of the Smart Grid, such as Smart Grid distribution devices.

Additionally, NERC's 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 CIP Reliability Standards apply to installed equipment and require security controls be applied to manage risk in the operation and maintenance of cyber assets. However, 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, NIST should integrate adequate cyber security protection, at all levels (device, application, network and system) in the development of a cyber security strategy for the Smart Grid that goes beyond the requirements of NERC CIP Reliability 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 a broader approach to prevent cyber security vulnerabilities on the Smart Grid in the overall cyber security framework. NERC's CIP Reliability Standards focus on protecting the integrity of the bulk power system rather than on components or specific functions. While NERC's CIP Reliability Standards require identification of bulk power system components that are material to the reliability of the bulk power system, they do not focus on the ability to serve customers on all elements of the bulk power system or on the protection of those elements. Therefore, NIST's cyber security strategy for the Smart Grid should integrate cyber security protection for those parts of the Smart Grid that the CIP Reliability Standards cannot protect.

NERC believes the cyber security strategy for the Smart Grid should focus on potential cyber security vulnerabilities of 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. NERC intends to work closely with NIST through the Cyber Security Coordination Task Group and the Smart Grid Interoperabilty Panel in the development of an overall cyber security strategy for the Smart Grid.

5. Chapter 3: NIST Presents a Logical Interface Analysis and Characterizes All of the Logical Interfaces with the Smart Grid. These Characterizations are Inadequate because NIST Does Not Specifically Analyze the Core

Components of the Smart Grid – a Task that is Essential in Ensuring the Reliability and Security of the Smart Grid.

In Chapter 3, NIST analyzes the interface diagrams for the six functional priority areas provided in the Smart Grid Framework Document,[30] and identifies the logical data flows within each interface diagram, identifying the security constraints and issues for each interface.[31] The logical interfaces in the six functional priority areas were allocated to one of fifteen different categories, and within each of these fifteen categories, the confidentiality, integrity and availability impact levels of data compromises at each interface was examined.[32] 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 include in Chapter 3 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

[30] *Id.* at p. 3.
[31] *Id.* at p. 15.
[32] *Id.*

to maintain bulk power system reliability. Accordingly, it will be essential to distinguish between core components and optimization functions.

For example, in Section 3.3, NIST examines the category of "[c]ontrol systems with high data accuracy and high availability, as well as media and compute constraints," and provides as an example systems that are "[b]etween SCADA and field equipment." NIST then goes on to examine the constraints and issues associated with this scenario. While an examination of the potential constraints and issues associated with this scenario is useful, NERC believes an additional category examining the core equipment should be included because only certain parts of "[c]ontrol systems with high data accuracy and high availability, as well as media and compute constraints" are core components. This additional analysis will provide the information that the industry needs to examine which equipment merely optimizes the Smart Grid, and which equipment is vital for a functioning electric grid. For example, the ability to keep SCADA systems running is a core requirement.

Once these core components are determined, an additional analysis of the "confidentiality," "integrity," and "availability" categories must be analyzed so that the industry understands which of these categories are core functions. Core functions will be those parts of the Smart Grid that *must* be preserved under a complete failure mode. Therefore, understanding what is core is essential to ensuring a grid safe from cyber security attacks.

For example, pages 22 and 23 of the Smart Grid Cyber Security Document describes the category "[b]ack office systems under common management authority," includes the subcategory "integrity," in which NIST states that the "[l]oss of integrity of data can cause power outages, including massive outages if meters are disconnected without authorization." NIST continues that the "[l]oss of integrity of data could cause safety hazards for utility personnel,

customer, and property." NERC believes these considerations could be expanded to include an analysis of the core functions. That is, NIST could include in its analysis an examination of the disconnection or *reconnection* of meters without authorization, because, from a power balancing perspective, while the loss of power to thousands of homes is significant, the industry must also consider the impacts of the reconnection happening too fast. If the disconnection or reconnection happens too fast and in a large scale, it will be extremely difficult to balance that system. Therefore, NERC encourages NIST to expand its view of the scenarios provided in Chapter 3 to examine the core functions. By doing so, if there is a core component or function, it will be known to the industry at the time or even before a potential incident. This will provide the industry with the necessary tools to prioritize the safety and preservation of the core components and functions over equipment that is for optimization purposes only. An examination of core components and functions will also help the industry develop a plan to bring those core components back online as quickly as possible in the event of a cyber security vulnerability.

While NERC believes the use cases provided in Chapter 3 are useful because they help the industry consider potential concerns associated with the Smart Grid, the impacts analyzed miss an important point that needs to 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. Additionally, some of the use cases analyzed in Chapter 3, 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, 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/ Michael J. Assante

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
michael.assante@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