

PREPARED STATEMENT OF MICHAEL J. ASSANTE
PRESIDENT AND CHIEF EXECUTIVE OFFICER
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS OF THE UNITED
STATES INC.

BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Technical Conference on
SMART GRID INTEROPERABILITY STANDARDS

January 31, 2011

January 31, 2011

Good afternoon, Chairman Wellinghoff, Commissioners, and staff. I want to thank the Commission for convening this technical conference on smart grid interoperability standards and for the opportunity to provide these remarks.

My name is Michael Assante. In addition to my experience as the Chief Security Officer at American Electric Power (AEP), I most recently served as the first Chief Security Officer of the North American Electric Reliability Corporation (“NERC”), which has been designated the Electric Reliability Organization (“ERO”) in the United States and much of Canada. Since departing NERC, I have remained active in efforts to enhance the security, survivability, and resilience of electric power systems in North America. I am providing comments based on my past experience associated with the challenges of developing industry standards and more limited experience involving the five families of standards before the Commission.

I believe properly developed technical standards will play an important role in establishing a strong foundation for future electric system reliability and security. The Commission properly identified areas that deserved high priority in the smart grid standards development process. These areas include two cross-cutting issues, system security and inter-system communication, and four key grid functionalities: wide-area situational awareness, demand response, electric storage, and electric vehicles. I recognize the growing desire, as significant investments are already being made, to adopt standards that will shape smart grid technologies to promote system interoperability and security. I fully believe we must achieve these important goals and that urgency in this matter is warranted, but I caution against allowing haste to overcome a deliberate and extensive review of these important guides that will be so crucial to the development of the future smart grid.

In my comments today, I will focus on both the security considerations and the standards consensus process associated with the five technical standards before the Commission at this time.

It is my strong belief that technical standards, particularly where the electric power system is concerned, must first and foremost do no harm. A successful standard must demonstrate that, if implemented in a prudent manner, it will result in outcomes that will not adversely affect the reliability or cybersecurity of the system, whether in part or in whole. Thinking through the real-world outcomes of proposed standards requires that many minds come to the table—from those that design the technology, to those that implement it, to those that must secure it.

The question of whether there is “sufficient consensus” that the five families of standards posted by the National Institute of Standards and Technology are ready for Commission consideration in a rulemaking proceeding is, therefore, and important one to ask. I would like to recognize up front the contributions and active involvement from important segments of the power industry, researchers, academics, and technology providers. From the onset, NIST has provided a valuable means for stakeholder input into the smart grid standards development process through formation of the Smart Grid Interoperability Panel (SGIP), a public-private partnership of 22 stakeholder groups supporting NIST in the ongoing coordination, acceleration and harmonization

January 31, 2011

of standards development for the smart grid. The distillation of such a complex topic as smart grid has benefited from the active participation of many industry segments. I am concerned however, that an insufficient number of experts in cybersecurity were engaged throughout the review process.

Even though the IEC process is well-established and technically sound, it, like many other efforts, is struggling to address the dynamic nature of cybersecurity. I have been disappointed with the low level of participation by cybersecurity experts in the original development, drafting, and approval of the family of IEC standards, as is highlighted by gaps and security principles that would benefit from greater clarity and correction. NIST's review, specifically the hard work of the Cyber Security Working Group (CSWG) Standards Subgroup, did identify areas to be addressed, but that effort also lacked consistent engagement by objective security experts.

Greater involvement by various domain security experts would further highlight potential areas of concern and gaps, as well as potential solutions. Over my career, I have been involved in many efforts that relied upon the generous contributions of individuals volunteering their time and expertise and know all too well how important it is to be respectful of their other commitments and responsibilities. Many security experts indicated to me that they were too busy working in their primary field or industry and found the process to be cumbersome and extremely time-consuming. I am also concerned that the process did not prioritize input from utilities that will be responsible for implementing, operating, and maintaining the technology in a secure manner.

These specific standards identify worthwhile technology targets that will certainly enhance efficiency and enable greater flexibility. For example, IEC 61850 substation architectures provide significant benefits, to include lower cost over the life of the system compared to existing architectures. These benefits, however, also introduce security concerns as critical functions and components would share a common network, common naming, and automatic point configuration; rely on peer-to-peer messaging; and would thus be more susceptible to data storms, setting changes, and malicious programming. Today, right or wrong, substations are designed to follow a virtually unlimited number of physical and cyber architectures. The amount of knowledge required to conduct a coordinated attack on the power system is thereby difficult to attain. Adding commonality to the design and architecture of these systems makes it much easier for an attacker to immediately understand his cyber "whereabouts" in a given location and to gauge the effects of his subsequent actions with a much higher degree of certainty. It is not always intuitive, but the idiosyncrasies of a large and diverse system developed over many years and operated by over 3,000 different entities have offered some risk reduction in requiring attackers to conduct discovery to formulate a deliberate non-opportunistic attack.

It is also important to consider the implications of field automation sharing networks for control and protection functions, which can make an attacker's task of causing damage in the physical world much easier. Some legacy industrial systems relied on physically separate and functionally independent control and protection systems that made it difficult to remotely manipulate system settings. This is significant as the removal of this physical separation and functional independence between control and protection systems introduces the opportunity for

January 31, 2011

an attacker to explore and manipulate the safety system to remove planned safeguards before misusing the control system to create a dangerous condition.

There is an important trade-off to consider between the benefit of achieving greater efficiencies by doing away with silos and leveraging shared network resources and the potential for increased vulnerability to a cyber threat from making more available to an attacker who gains access to the network. The benefits might be deemed to outweigh the potential risks, but this requires a greater scrutiny of the necessary security approaches to manage those risks.

As a security professional I am always challenged to measure the risk associated with designs and specifications on paper without having a detailed reference or model to evaluate. I have worked with engineers and security assessors that have implemented systems that followed specific portions of these standards. Each of them referred to the standards as guides that failed to offer demonstrated implementations to inform technology and configuration decisions. The standards have been criticized for not addressing existing and new substation architectures, failing to map with more widely accepted implementations and legacy systems, and not being harmonized with existing initiatives to include synchrophasor efforts.

Many experts have argued that there is a concerning lack of security features being built into existing smart grid systems. The technology provider community has been criticized for developing and deploying solutions that have not been designed with a strong security architecture and lack important security features, including strong authentication, event logging, and forensics capabilities, which are necessary to analyze attacks. In my opinion, the existing standards do not make sufficient progress in establishing paths to significantly enhance the security of electricity delivery systems. In some instances these standards simply call on system owners to implement security features that counter, within appropriate user and cost constraints, certain key threats, specifically denial of service and illegitimate use.

The greatest concern is raised by engineers that have characterized the standards as being based more on experimentation than on implemented field experience, particularly in the U.S. Security challenges are always complicated by tough trade-off decisions that are made when trying to implement a system in a non-laboratory environment. The lack of implemented systems relative to the number of design options certainly makes it difficult, if not impossible, to gauge whether the standards will result in outcomes that will not adversely affect the reliability or cybersecurity of the electric power system. For example the IEC 61850 family of standards explains the need for confirmation of a control message response, but does not identify appropriate security to address integrity and confidentiality concerns for the response. It is also interesting to note that IEC 61850 currently has little penetration in the U.S. market. The most popular substation standard, DNP-3, was not one of the standards being provided by NIST.

We must strive to avoid technical standards that either falls short of requiring a solid core of built-in security features or possess known security challenges without identified security solutions. At AEP, I learned the tough lesson of having to bolt on additional protective measures after a system had been developed. As a former asset owner, I would rather set a higher bar for systems in the design and development phase, as it is far more effective and cost efficient to deal with the security challenges, such as those that have been identified by the NISTIR 7628

January 31, 2011

Guidelines for Smart Grid Cyber Security and by the NIST Risk Management Framework, before systems have been installed and are operational.

As a former regulator, I also know all too well what happens when insufficient standards are adopted and the problems created in attempting to enforce compliance and trying to fix those standards while they are being implemented. Even the many entities acting in good faith faced difficulty in interpretation and implementation—and I have seen the same issues already beginning to arise here. I will remain uncomfortable with the current NIST standards until model systems built using the existing standards are tested in both laboratory and field settings. There are too many questions left at the discretion of implementers, integrators, and asset owners with inadequate guidance and a lack of practical and demonstrated security approaches to inform their decisions. Furthermore, the standards under consideration contain many decision branches and configuration decisions that would certainly introduce difficulties to achieving ready-made interoperability.

Efforts to modernize our nation's electric power infrastructure through the overlay of two-way digital communications and highly-automated digital control (to create the "smart grid") are based on the desirable promise of greater energy efficiency and system performance. Indeed, the smart grid may well pave the way to an entirely new way of considering electricity supply and demand. Of course, more technology typically adds more complexity and interconnectedness, which tend to increase system fragility and vulnerability to perturbations. We should continue to seek progress, but also recognize the need to close the gaps in the software and system engineering foundations necessary to ensure that new smart grid functionality will be secure, safe, survivable, reliable, and resilient.

I don't believe my concerns are insurmountable, but they should be addressed before setting a precedent by adopting the standards in their current form. There are several approaches that could be considered to improve the standards, to include remanding the technical standards until security is uniformly addressed or direct necessary addendums to address concerns and provide credible security guidance.

Efforts should be made to establish an agreed-upon set of review criteria by type of technical standard to evaluate its impact on system security. These reviews should include an evaluation of pilot implementations where possible. I am not necessarily advocating a long and drawn-out process and surely recognize the value in setting direction while the opportunity to do so still exists. I would ideally like to see an intensive but timely review process undertaken, utilizing the resources at utility test beds and technology labs across the country. The existing review process would benefit from engaging a more diverse group of cybersecurity experts to include individuals working in other sectors, particularly in the field of control system cyber security, and in the field of general information technology.

Again, I appreciate the opportunity to speak before you today and commend the Commission and NIST's efforts to tackle this important and growing issue. I would be pleased to answer any questions you may have.

January 31, 2011

Respectfully submitted,

/s/ Michael Assante

Michael Assante
President and Chief Executive Officer

National Board of Information Security
Examiners of the United States, Inc.
2184 Channing Way, #304
Idaho Falls, ID 83404
(208) 557-8026
(973) 860-0921 – facsimile
michael.assante@nbise.org