1200 G Street, NW
Suite 500
Washington, DC 20005

P: 202-628-6380
F: 202-393-5453
W: www.atis.org

December 1, 2009

Ms. Annabelle Lee
National Institute of Standards
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899-8930

Re: General Comments NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements in Docket No. 0909301329-91332-01

Dear Ms. Lee:

The Alliance for Telecommunications Industry Solutions (ATIS) appreciates the opportunity to offer comments on the initial draft of the (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements (NIST Smart Grid Cyber Security Requirements). Given the critical and interconnected role that the information technology and communications (ICT) sector plays in supporting the implementation of Smart Grid, ATIS strongly supports NIST's efforts to identify and assess the security vulnerabilities and design in security requirements at the design phase of the Smart Grid.

The purpose of these comments is to make NIST's Smart Grid Cyber Security Coordination Task Group (CSCTG) aware of ATIS' standards development efforts and other work related to cyber security in the ICT sector which may be helpful as the CSCTG refines this initial draft of its NIST Smart Grid Cyber Security Requirements. ATIS is very interested in the Smart Grid implementation and recently submitted comments[1] to the NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft), in which ATIS is listed as one of the collaborating standards development organizations. Additionally, this past summer ATIS participated in NIST workshops aimed at developing the roadmap for Smart Grid standards.

[1] Letter to Dr. George W. Arnold, National Coordinator, Smart Grid Interoperability, National Institute of Standards, Commenting on the *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)* (November 9, 2009).

A. Background

ATIS is a global standards development and technical planning organization committed to providing leadership for, and the rapid development and promotion of worldwide technical and operations standards for information, entertainment and communications technologies using a pragmatic, flexible and open approach. ATIS is accredited by the American National Standards Institute (ANSI), a private, non-profit organization that administers and coordinates the U.S. voluntary standards and conformity assessment system.

ATIS' membership is diverse, including all stakeholders from the ICT industry – wireline and wireless service providers, equipment manufacturers, competitive local exchange carriers, data local exchange carriers, providers of commercial mobile radio services, broadband providers, software developers, consumer electronics companies, digital rights management companies, and internet service providers.

Nearly 600 industry subject matter experts from more than 250 ICT companies work collaboratively in ATIS' 18 open industry committees. The ATIS committees focus on a broad range of priorities for the ICT industry, including network architectures and platforms, the ordering and billing of services, E-911, cyber security, the reliability and interoperability of current and next generation technologies, the seamless delivery of converged wireline and wireless services such as IPTV over multimedia platforms, and the networks of the future.

B. Open and Accessible Standards

While ATIS supports NIST's efforts to develop cyber security standards related to Smart Grid, ATIS is concerned that statements in Appendix D.4 Openness and Accessibility of Smart Grid Standards could be misconstrued to imply that simply because there is a charge for a standard that the standard is not "accessible." Neither openness nor accessibility demands that documents be made available without charge. Many standards development organizations, including ATIS, recover the costs of their activities through nominal document fees and such fees are essential to the development of standards. The terms "open" or "openness" describe the collaborative, balanced and consensus-based approval process used to develop standards. This process includes opportunity for broad-based public review and comment as well as opportunity for appeal if due process principles are not respected. ATIS follows such processes and promulgates open standards that are publically available and accessible.

ATIS agrees that "secretly developed" algorithms or protocols may be a cause for concern. However, ATIS does not believe that standards developed through the open standards development process described above require either that the documents be made available for free or that the intellectual property (IP) owners must relinquish their rights. Instead, ATIS believes that it is important to balance the interest of those who will implement such standards with the interest of the IP owners.

C. Model for Assessing Telecommunications Network Circuit Diversity In Relation to Smart Grid Implementation

According to this initial draft of the NIST Smart Grid Cyber Security Requirements, cyber security refers to "the protection required to ensure confidentiality, integrity, and availability of the electronic information communication system."[2] It is clear to see that the ICT sector will be integral to the implementation of the Smart Grid.

Thus, assessing telecommunications network circuit diversity should be a component of the overall cyber security evaluation of Smart Grid. To ensure that the telecommunications infrastructure that supports Smart Grid is resilient in the event of physical destruction of network facilities (central offices, outside plant, etc.), telecommunications circuits that provide key operations must be redundant and have diverse pathways. The ATIS National Diversity Assurance Initiative (NDAI) (report published in February 2006), provides a comprehensive overview of the process involved to determine if telecommunications circuits are truly diverse at the street level. The NDAI effort was conducted to evaluate diversity assurance for the Federal Reserve Bank. This assessment model can be readily applied to evaluate circuit diversity in other sectors, including energy.

D. ATIS' Cyber Security Related Standards and Work Effort

ATIS forums, including the Chief Information Officer (CIO) Council, the Optical Transport and Synchronization Committee (OPTXS), and the IPTV Interoperability Forum (IIF), are engaged in developing work products related to cyber security.

ATIS' Chief Information Officer (CIO) Council, which provides a venue for CIO-level executives from among the largest service provider companies to identify and discuss information technology (IT) issues, is addressing the IT impacts related to cyber security. The ATIS CIO Council is currently examining the Cybersecurity Act of 2009[3] and has formed an Enterprise Risk Management (ERM) Working Group to explore three specific areas related to the cyber security legislation, including the potential impacts to carriers, technical implications, and providing public comments.

The cyber security aspects of Smart Grid will also be affected by the timing and synchronization performance. The ATIS Optical Transport and Synchronization Committee (OPTXS) develops standards that focus on telecommunication equipment that transport voice, data, and video over copper and fiber and its OPTXS-Synchronization (SYNC) Subcommittee concentrates on the synchronization aspects including accurate generation and distribution of timing (time/frequency) signals. OPTXS-SYNC may add value in the evaluation of security risks caused by modifications that violate Ethernet layering functions. In addition, OPTXS-SYNC

---

[2] *See* NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements (September 2009).

[3] Cybersecurity Act of 2009, S.773, 111th Cong.

would be able to assist in evaluating performance impacts caused by security countermeasures in relation to their suitability especially for packet-based timing applications.

ATIS notes that Appendices D.17 and D.24 of the NIST Smart Grid Cyber Security Requirements highlight the importance of developing key management standards to Smart Grid cyber security. ATIS' IPTV Interoperability Forum (IIF), which enables the interoperability, interconnection, and implementation of IPTV systems/services, has published several standards involving authentication protocols and security robustness relative to IPTV. These standards include: *ATIS-0800024 Security Robustness Rules Interoperability Specification* and *ATIS-08000014 Secure Download and Messaging Interoperability Specification*. Some of the concepts contained in these documents may be applicable to the ongoing work in NIST on Smart Grid.

Conclusion

ATIS strongly supports NIST's effort to address the security requirements of the Smart Grid upfront during the architectural design phase. Having worked with the communications, banking and financial industries to assess critical telecommunications infrastructure vulnerabilities, ATIS believes that it is paramount that NIST's implementation of a modernized electricity transmission and distribution system addresses the security, reliability and interconnectedness of the ICT and energy sectors.

Respectfully submitted,

By: 

Thomas Goode,
General Counsel

By: 

Deirdre Cheek,
Attorney

Alliance for Telecommunications Industry Solutions
1200 G Street, N.W., Suite 500
Washington, D.C. 20005

Its Attorneys