PREPARED STATEMENT OF DONNA F. DODSON

CHIEF CYBERSECURITY ADVISOR AND DIRECTOR OF THE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE AT THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Commissioner-Led Technical Conference on
RELIABILITY

JUNE 1, 2016

Good afternoon, Chairman Bay, Commissioners LaFleur, Clark and Honorable, and fellow panelists. Thank you for the opportunity to join you today and speak about security and resilience of the electric grid. My name is Donna Dodson and I am the Chief Cybersecurity Advisor for the National Institute of Standards and Technology (NIST), Associate Director of Cybersecurity within the Information Technology Laboratory (ITL), and the Director of NIST's National Cybersecurity Center of Excellence (NCCoE).

NIST is a non-regulatory federal agency within the U.S. Department of Commerce, specifically focused on promoting U.S. economic competitiveness. The NIST laboratories work at the frontiers of measurement science to ensure that the U.S. system of measurements is firmly grounded on sound scientific and technical principles. Today, the NIST Laboratories address increasingly complex measurement challenges, ranging from the very small nanoscale devices to the very large vehicles and buildings, and from the physical, renewable energy sources, to the virtual, cybersecurity and cloud computing. As new technologies develop and evolve, NIST's measurement research and services remain central to innovation, productivity, trade, and public safety.

ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. In the area of cybersecurity, NIST has worked with Federal agencies, industry, and academia since 1972, starting with the development of the Data Encryption Standard, when the potential commercial benefit of this technology became clear. NIST's role, to research, develop and deploy information security standards and technology to protect the Federal government's information systems against threats to the confidentiality, integrity and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. § 3541 et seq.) and recently reaffirmed in the Federal Information Security Modernization Act of 2014 (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure

We employ collaborative partnerships with our customers and stakeholders to take advantage of their technical and operational insights and to leverage the resources of a global community. These collaborative efforts and our private sector collaborations in particular, are constantly being expanded by new initiatives, including in recent years through the National Strategy for Trusted Identities in Cyberspace (NSTIC), the National Cybersecurity Center of Excellence (NCCoE), in implementation of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" and the National Initiative for Cybersecurity Education (NICE).

My comments today will focus on NIST's research, development and outreach to provide standards and guidelines, mechanisms, tools, metrics, and the effective application of these resources to protect the U.S.'s information and information and industrial control systems.

The Cybersecurity Act of 2015, passed in late December as part of the Fiscal 2016 omnibus appropriations measure, was developed to provide long-sought liability protection to entities that share cyber threat indicators. The Cybersecurity Act of 2015 addresses mechanisms for cybersecurity information sharing and includes measures designed to strengthen federal cybersecurity.

Cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats. Examples of cyber threat information include indicators such as system artifacts or observables associated with an attack, security alerts, threat intelligence reports, and recommended security tool configurations.

Through the exchange of cyber threat information with other sharing community participants, organizations can leverage the collective knowledge, experience, and capabilities of a sharing community to gain a more complete understanding of the threats they may face. Using this knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation

strategies. By correlating and analyzing cyber threat information from multiple sources, an organization can enrich existing information and make it more actionable. This enrichment may be achieved by independently confirming the observations of other community members, and by improving the overall quality of the threat information through the reduction of ambiguity and errors.

Members of a sharing community who receive information and subsequently remediate a threat also confer a degree of protection to other community members (even those who may not have received or acted upon the cyber threat information) by impeding the threat's ability to spread. NIST encourages greater sharing of cyber threat information among organizations, both acquiring threat information from other organizations and providing internally-generated threat information to other organizations.

In April 2016, NIST released the second draft of Special Publication (SP) 800-150, Guide to Cyber Threat Information Sharing, for public comment. This draft provides guidelines for establishing, participating in, and maintaining cyber threat information sharing relationships. The goal of the publication is to provide guidelines that help improve cybersecurity operations and risk management activities through safe and effective information sharing practices. The public comment period for this publication closed on May 24, and the team is working to assess, analyze and address the comments received to move toward final publication.

The threat to our systems and information is dynamic and rapidly evolving; we must build equally agile and responsive capabilities. In partnership with federal agencies and other stakeholders, NIST has developed standards, guidelines, and recommendations to provide a standardized and repeatable framework, the NIST Risk Management Framework, for managing risks to Federal information and IT systems.

The Risk Management Framework provides a structured, yet flexible, approach for managing the risk resulting from using information systems to achieve the mission and business processes of an organization. The risk management concepts are intentionally broad-based with the specific details of assessing risk and employing appropriate risk mitigation strategies provided by supporting NIST information security standards and guidelines. This approach allows for implementation of cost-effective, risk-based information security programs. It establishes a level of security due diligence for Federal agencies and contractors supporting the Federal government. It creates a consistent and cost-effective application of security controls across an information technology infrastructure and a consistent, comparable, and repeatable security control assessment. When implemented, it gives an organization a better understanding of enterprise-wide mission risks resulting from the operation of its information systems.

It is important to note that the impact of NIST's activities extend beyond providing the means to protect Federal IT systems. NIST is tasked with the key role of coordinating Federal agency use of voluntary consensus standards and participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. Working with other Federal agencies such as the Departments of Defense, State and Homeland Security, we coordinate positions on standards issues and priorities with the private sector through consensus standards such as American National Standards Institute (ANSI), the Joint Technical Committee 1 (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunications Union's Standardization Sector (ITU-T).

Cybersecurity standards provide the foundations for the public trust that is essential to our realization of the national and global productivity and innovation potential of electronic business and its attendant economic benefits. Many organizations voluntarily follow NIST standards and guidelines, reflecting their wide acceptance throughout the world. NIST's partnership with industry to develop, maintain, and implement voluntary consensus standards related to cybersecurity best ensures the interoperability, security, and resilience of the global infrastructure needed to make us all more secure. It also allows this infrastructure to evolve in a way that embraces both security and innovation – allowing a market to flourish to create new types of secure products for the benefit of all Americans.

In February 2014, NIST issued the Framework for Improving Critical Infrastructure Cybersecurity (Framework)[1] in accordance with Section 7 of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."[2] The Framework, created through collaboration with industry, government, and academia, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk. Since the release of the Framework, NIST has strengthened its collaborations with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders to raise awareness about the Framework, encourage use by organizations across and supporting the critical infrastructure, and develop implementation guides and resources. The Framework continues to be voluntarily implemented by industry and adopted by infrastructure sectors, which is contributing to reducing cyber risks to our Nation's critical infrastructure.

Pursuant to the Cybersecurity Enhancement Act of 2014, NIST has convened meetings with regulators to discuss application of the Framework within the cyber ecosystem, and the need for the Framework to remain a voluntary methodology, adaptable to the critical infrastructure risk and mission objectives. NIST is also an advisory member of the Cybersecurity Forum for Independent and Executive Branch Regulators. The forum was chartered to increase the overall effectiveness and consistency of regulatory authorities' cybersecurity efforts pertaining to U.S. Critical Infrastructure. In all of these interactions, NIST continues to communicate the merits of the voluntary Framework as an organizational and communication tool to better manage cybersecurity risk.

Under the Energy Independence and Security Act of 2007 (EISA), NIST was assigned the "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems." [EISA Title XIII, Section 1305]. Coordination is a key word in that tasking. Our approach focuses on our internal measurement research programs and collaboration with organizations such as the Smart Grid Interoperability Panel (SGIP) and others to improve the interoperability, security and resilience of the electric grid. Developed through this coordination strategy, NIST's Framework and Roadmap for Smart Grid Interoperability Standards (NIST SP1108) and NIST's Guidelines for Smart Grid Cybersecurity (NISTIR 7628) were first published in 2010 with the most recent revisions being released in 2014.

NIST has recognized the potential for electromagnetic interference (including geomagnetic disturbances) to affect grid operations. Due to an ever increasing density of electromagnetic emitters (radiated and conducted, intentional and unintentional) in the environment, the new equipment must have adequate immunity in order to function consistently and reliably, be resilient to major disturbances, and coexist with other equipment.

Within our Communications Technology Laboratory, we conduct research to develop measurement methods, interference models, and metrics to improve Electromagnetic Compatibility (EMC) testing for communications and other systems deployed in smart grid (SG) environments; and to provide technical input to smart grid EMC standards activities to meet performance and interoperability requirements. This research complements work within the Radio Frequency Technology Division in broadband wireless systems, homeland security, EMC and electromagnetic field metrology.

Within our standards coordination role for smart grid interoperability standards, we have worked previously to add a working group within the SGIP, originally chaired by a NIST electromagnetics expert, to identify electromagnetics interference issues and develop strategies to implement effective electromagnetic compatibility to help mitigate risks.

[1] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
[2] https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

This SGIP Electromagnetic Interoperability Issues Working Group (EIIWG) was formed in 2010 to "investigate enhancing the immunity of Smart Grid devices and systems to the detrimental effects of natural and man-made electromagnetic interference, both radiated and conducted. The focus is to address electromagnetic compatibility (EMC) issues and to develop recommendations for the application of standards and testing criteria to ensure EMC for the Smart Grid, with a particular focus on issues directly related to interoperability of Smart Grid devices and systems, including impacts, avoidance, generation and mitigation of and immunity to electromagnetic interference."

The primary goal for the SGIP EIIWG is "to identify and focus on the critical parts of the Smart Grid and develop a strategy to implement effective EMC, including standards, testing and conformity assessment, with particular focus on issues directly affecting interoperability of Smart Grid devices and systems." This working group has worked steadily to meet these goals and has successfully and significantly contributed to the awareness and understanding of the EMC issues that may affect the ability of Smart Grid devices to interoperate. Their work has included a comprehensive review of EMC issues for the Smart Grid as documented in the white paper SGIP-2012-005, V1.0, "Electromagnetic Compatibility and Smart Grid Interoperability Issues," as well as other more targeted standards activities and recommendations.

We at NIST recognize that we have an essential role to play in helping industry, consumers and government to counter cyber threats. We are extremely proud of our role in establishing and improving the comprehensive set of cybersecurity technical solutions, standards, guidelines, and best practices and the robust collaborations with our Federal government partners, private sector collaborators, and international colleagues. NIST sits at the nexus of science and industry, conducting cutting-edge, world-class measurement science and developing standards that allow industry to innovate and compete in the global economy.

Thank you for the opportunity to speak today. I would be happy to answer any questions you may have.