Testimony of

Cita M. Furlani
Director

Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Joint Hearing
Before the
United States House of Representatives
Committee on Science and Technology
Subcommittee on Technology and Innovation and
Subcommittee on Research and Science Education

"Protecting Information in the Digital Age: Federal Cybersecurity Research and Development Efforts"

May 25, 2011

Chairmen Quayle and Brooks, Ranking Members Wu and Lipinski and Members of the Subcommittees, I am Cita M. Furlani, Director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in protecting information in the digital age.

As Secretary of Commerce Gary Locke said at the White House during the launch of the U.S. International Strategy for Cyberspace: "To preserve and even improve on people's confidence in cyberspace, we need an environment that not only rewards innovation and empowers entrepreneurs, but one that also is constantly improving upon the integrity of the interactions that take place online." NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life is well positioned to support that goal.

As one of the major research components of NIST, the Information Technology Laboratory (ITL) accelerates, through standards, tests and metrics, the development, deployment and use of secure, usable, interoperable and reliable information systems that enable American businesses to be more innovative competitive. ITL enables world-class measurement and testing through research innovations in the areas of computer science and systems engineering, mathematics, and statistics. We balance our research portfolio to be responsive to pressing national priorities while pursuing research necessary to meet future challenges in measurement science and technology. Our R&D agenda focuses on the following broad program areas: cloud computing, complex systems, cybersecurity, biometrics, health information technology, National Initiative for Cybersecurity Education (NICE), National Strategy for Trusted Identities in Cyberspace (NSTIC), quantum information, pervasive information technology, security automation, smart grid, virtual measurement systems, and voting standards.

ITL addresses technical challenges through an integrated, multidisciplinary and systems approach that emphasizes collaboration with other NIST organizations, the Department of Commerce, other government agencies, the U.S. private sector, standards development organizations, and other national and international stakeholders. Our rich programmatic diversity derives from our mission and mandates like the Federal Information Security Management Act (FISMA), which charges ITL to develop cybersecurity standards, guidelines, and associated methods and techniques. Charged under other legislation, such as the USA PATRIOT Act, the HITECH Act and the Help America Vote Act, we are addressing major challenges faced by the nation in the areas of homeland security, health IT and electronic voting.

Overview of NIST Cybersecurity Activities

As you are aware, beginning in the early 1970s with enactment of the Brooks Act, NIST has developed standards to support federal agencies' information assurance requirements. Through FISMA, Congress again reaffirmed NIST's leadership role in developing standards for cybersecurity. FISMA provides for the development and promulgation of Federal Information Processing Standards (FIPS) that are "compulsory and binding" for Federal computer systems. The responsibility for the development of FIPS rests with NIST, and the authority to promulgate mandatory FIPS is given to the Secretary of Commerce. Section 303 of FISMA states that NIST shall:

- have the mission of developing standards, guidelines, and associated methods and techniques for information systems;
- develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems; and
- develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

NIST's mission in cybersecurity is to work with federal agencies, industry, and academia to research, develop and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity and availability of information and services. Consistent with this mission and with the recommendations of the President's *Cyberspace Policy Review*, NIST is actively engaged with private industry, academia, non-national security federal departments and agencies, the intelligence community, and other elements of the law enforcement and national security communities in coordination and prioritization of cybersecurity research, standards development, standards conformance demonstration and cybersecurity education and outreach activities. Research activities range from innovations in identity management and verification, to metrics for complex systems, to development of practical and secure cryptography in a quantum computing environment, to automation of discovery and maintenance of system security configurations and status, to techniques for specification and automation of access authorization in line with many different kinds of access policies.

NIST addresses cybersecurity challenges throughout the information and communications infrastructure through its cross-community engagements. Enabled by Congressional funding increases in 2002 and in response to FISMA, NIST is responsible for establishing and updating, on a recurring basis, the federal government risk management framework and cybersecurity controls. The national security community, a number of state governments and major private sector organizations are also adopting the risk management framework and cybersecurity controls designed by NIST. NIST is engaging industry to harmonize standards conformance requirements to align with industry business models and system development practices. NIST is also playing a leading security role in supply chain risk management, Health Information Technology, the Smart Grid, biometrics/face authentication, cybersecurity education and training beyond the federal government, next generation voting systems, and cloud computing. NIST is working with the intelligence and counterterrorism communities to facilitate cross sector information sharing among federal, state and local government organizations.

Recognizing the importance of security-related standards beyond the federal government, NIST leads national and international consensus standards activities in cryptography, identity management, biometrics, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing.

Included in the scope of NIST cybersecurity activities are the usability of systems such as voting machines, electronic health records and software interfaces; network security, including standards and tests for Internet Protocol version 6, Domain Network Security (DNSSec), and

wireless network protocols; research in mathematical foundations to determine the security of information systems; the National Software Reference Library, computer forensics tool testing, and mobile device forensics; software assurance metrics, tools, and evaluation; approaches to balancing safety, security, reliability, and performance in SCADA and other Industrial Control Systems used in manufacturing and other critical infrastructure industries; technologies for detection of anomalous behavior, quarantines; standards, modeling, and measurements to achieve end-to-end security over heterogeneous, multi-domain networks; biometrics evaluation, usability, and standards (fingerprint, face, iris, voice/speaker, multimodal biometrics) and an international competition for a next generation Secure Hash Algorithm (SHA-3).

NIST Role in Cyberspace Policy Review Activities
NIST is actively participating in meeting the objectives of several of the near- and mid-term action plan activities from the Cyberspace Policy review.

National Initiative for Cybersecurity Education
- Cyberspace Policy Review Near-Term Action Item 6: Initiate a national public awareness and education campaign to promote cybersecurity
- Cyberspace Policy Review Mid-Term Action Item 3: Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy
- Cyberspace Policy Review Mid-Term Action Item 4: Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.

The National Initiative for Cybersecurity Education (NICE) represents the evolution of the Comprehensive National Cybersecurity Initiative (CNCI) work on cybersecurity education. The scope of the initiative has been expanded from a federal focus to a broader national focus. NIST has assumed the overall coordination role for the effort, and is finalizing a strategic framework and a tactical plan of operation to support that framework. This expansion and the overall coordination role by NIST are in response to the President's priorities as expressed in Chapter II, *Building Capacity for a Digital Nation*, of the President's *Cyberspace Policy Review*.

NIST is currently readying the NICE strategic plan for public review, which should be available this summer. The strategic plan describes the goals and objectives that support the NICE Vision: *a secure digital nation capable of advancing America's economic prosperity and national security in the 21st century through innovative cybersecurity education, training, and awareness on a grand scale.*

NIST's NICE Team is working to unify and coordinate federal resources to enable the larger national effort to improve cybersecurity awareness, education, and training for the entire country. This effort is targeted to all U.S. citizens of all ages, and all types of professions whether it be academia, federal/state/local government, business partners (small-medium to large size businesses/companies), and local community groups. NICE is comprised of four components.

- Component 1: National Cybersecurity Awareness Campaign, encouraging a national culture of security in cyberspace; lead agency Department of Homeland Security (DHS), supported by Department of Education (ED), National Science Foundation (NSF),

Department of Defense (DoD), Office of the Director of National Intelligence (ODNI) and others as identified.

- Component 2: Formal Cybersecurity Education, enabling a broader pool of skilled workers for a cyber-secure nation; lead agencies DoED and NSF, supported by Office of Personnel Management (OPM), DHS, National Security Agency (NSA) and others as identified (e.g., Department of Labor)
- Component 3: Cybersecurity Workforce Structure, defining cybersecurity jobs, attraction, recruitment, retention, and career path strategies; lead agency DHS and supported by OPM.
- Component 4: Cybersecurity Workforce Training and Development, enabling the development and maintenance of an unrivaled cyber workforce; lead agencies DHS, DoD and ODNI, supported by OPM, DoED, NSF, and others as identified.

In addition, NIST co-chairs the Networking and Information Technology Research and Development (NITRD) Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW) Coordinating Group Education Team. The NITRD SEW Education Team was recently established to focus on workforce development, training, and education needs arising from the growing demand for productive information technology-skilled workers and the role of innovative IT applications in education and training. The group is currently developing a draft set of priority federal research areas in education and IT.

International Cybersecurity Policy Framework

- Cyberspace Policy Review Near-Term Action Item 7: Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
- Cyberspace Policy Review Mid-Term Action Item 12: Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies

To support the U.S. Government's international cybersecurity policy framework and strengthen our international partnerships, NIST and the National Security Agency lead an interagency activity to establish strategic objectives in pursuing the development of timely, technically sound international voluntary consensus cybersecurity standards. This includes commitment to the development of an international standards framework that:

- Ensures the availability of standards that promote security and resiliency for all U.S. information systems;
- Specifies performance criteria rather than detailed design criteria;
- Is open to innovation; and
- Discourages barriers to international trade.

Game Changing Technologies

- Cyberspace Policy Review Near-Term Action Item 9: In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience,

and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.

NIST is an active member in the groups that coordinate the cybersecurity research and development agenda for federal agencies. The NITRD Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), co-chaired by NIST, coordinates research and development to prevent, resist, detect, respond to, and/or recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer- and network-based systems. The Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group works in parallel to the CSIA IWG to coordinate classified cybersecurity R&D. Representatives from both of these groups participate together in the Senior Steering Group (SSG) for CSIA R&D, to actively share cybersecurity R&D information across the policy, fiscal, and research levels of the Government.

In May 2010, the CSIA IWG released its "Cybersecurity Game-Change Research & Development Recommendations,"[1] identifying three primary R&D themes to motivate future Federal cybersecurity research activities: (a) Moving Target, (b) Tailored Trustworthy Spaces, and (c) Cyber Economic Incentives. These themes are designed to inspire Federal and private cybersecurity researchers to discover novel solutions to increase the nation's cybersecurity protections. The NITRD CSIA IWG is currently developing a "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program."

Many of NIST's research activities include standards and technologies that will address the three R&D themes recommended by the CSIA IWG, including, but not limited to,

- Multi-Factor Authentication methods
    - NIST has successfully initiated an international standards project on anti-spoofing/liveness detection within ISO/IEC JTC 1 SC 37 (Biometrics). This is the first standards projects in this field, with the goal of strengthening the security of biometrics as an authentication factor for unattended applications. NIST is leading an international "team" of co-editors and has completed the first official working draft.
    - On March 31, NIST released results from the latest in its series of tests of fingerprint minutiae match-on-card (MOC) implementations. The report, NIST Interagency Report 7477, Revision II, details results for 17 MOC implementations submitted by 12 fingerprint-provider card-provider teams. The study shows that there are now five implementation providers that can meet the error rate requirements for Homeland Security Presidential Directive/HSPD-12 Personal Identify Verification (for biometric matching off card) while being able to process the comparison on a smartcard. This is a great example of successful standards and testing work to provide multi-factor authentication that is a privacy-enhancing solution.
    - NIST is collaborating with OASIS, ANSI/INCITS M1 and ISO JTC 1 SC 37 in developing web services protocols to enable the use of biometrics as a second factor for remote authentication of users for applications requiring higher levels of

[1] The full document is available at http://nitrd.gov/PUBS/CSIA_IWG_%20Cybersecurity_%20GameChange_RD_%20Recommendations_20100513.pdf

assurance. Biometrics and Web services may be combined to enhance mobile identification and remote authentication capabilities.

- Foundations of Measurement Science for Information Systems
    - Developing measurement and modeling techniques needed to enable the characterization, prediction, and control of the security of dynamic, large-scale interconnected information systems
- Emerging Virtual Technologies
    - Implementing a cloud computing and virtualization test environment to evaluate the security of virtualization techniques and the cloud computing systems and to develop ideas to mitigate security vulnerabilities in virtualized and cloud systems.
    - Leverage the test environment to support some of the Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) use cases by implementing a proof of concept for supporting the NIST 800-53 security control requirements for low and moderate impact baseline to a cloud computing service model such as infrastructure as a service reference implementation, which includes typical virtual workloads running on commercial hypervisors.
    - Define some typical use cases involving migrating virtual workloads from a private cloud to a public or community cloud while demonstrating compliance with the security and audit requirements.
- Usability of Security
    - Developed an in-depth interview instrument to explore users' perception of online risk, trust, privacy, and their knowledge of computer security terms and mechanisms. The goal of this effort is to understand user's mental models in order to assist in computer security education and training.
    - Completed the analysis of the password survey that was performed at NIST. Now analyzing the survey results from all of the Bureaus with the Department of Commerce; the survey closed at the end of April 2011.
    - Preparing to implement a second usability pilot based on the lessons learned with the Homeland Security Presidential Directive/HSPD-12 Personal Identify Verification (PIV) pilot at NIST.
    - Planning studies to evaluate the tradeoff of error rates in the human limitation between memory and typing and the complexity of the password.
- Quantum Computing
    - Researching cryptographic algorithms for public key-based key agreement and digital signatures that are not susceptible to cryptanalysis by quantum algorithms. Results are expected to be submitted to relevant standards development organizations.
- Mobile Handheld Device Security and Forensics
    - Developing tests and methodologies that will improve the security of mobile devices and enable the advancement of the state of the art in mobile device forensics.
- Security for Pervasive Systems and Grid Computing
    - Investigating trust management frameworks, protocols, and application programming interfaces for generalized pervasive systems security functions.

National Strategy for Trusted Identities in Cyberspace

- Cyberspace Policy Review Near-Term Action Item 10: Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.
- Cyberspace Policy Review Mid-Term Action Item 13: Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.

Under the leadership of the National Cybersecurity Coordinator, a multi-agency team, of which NIST was a substantial partner, created "The National Strategy for Trusted Identities in Cyberspace," which laid out the vision for individuals and organizations to be able to utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. The Strategy calls for a National Program Office to facilitate the carrying out of the Strategy and the development of interoperable technology standards and policies — an "Identity Ecosystem" — where individuals, organizations, and underlying infrastructure — such as routers and servers — can be authoritatively authenticated. The goals of the Strategy are to promote private sector capabilities for protecting individuals, businesses, and public agencies from the high costs of cyber crimes like identity theft and fraud, while simultaneously helping to ensure that the Internet continues to support innovation and a thriving marketplace of products and ideas in a privacy enhancing manner.

The National Program Office (NPO), to be established within the Department of Commerce, will coordinate the federal activities – including coordination of cooperative public/private efforts - needed to implement NSTIC. The office will be led by NIST with activities involving public policy development and privacy protections to be led by the National Telecommunications and Information Administration. The NPO will have full access to NIST technical expertise, both in the development and acceptance of broad consensus-based standards. NIST has been actively involved in the development and interoperability of secure identity management for many years and recently initiated research into how to make such identity schemes easy to use and hard to misuse.

NIST has hired an internationally recognized expert in identity management to manage the establishment of the NSTIC NPO. NIST has also announced the first in a series of workshops to collect public comments on possible private-sector led governance structures for the Identity Ecosystem. This first workshop will be held June 9-10, 2011 in Washington, D.C. Finally, NIST is working with others in the Department of Commerce to develop and release a Notice of Inquiry to achieve even greater public comment on the issue of governance.

Risk Management Framework

- Cyberspace Policy Review Mid-Term Action Item 6: Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.

NIST has produced Special Publication 800-34 "Contingency Planning Guide for Federal Information Systems" to assist with planning for system recovery and is currently working on

Special Publication 800-30 revision 1, "Risk Management Guide," which will provide guidance to agencies in threat identification, threat modeling, and threat metrics for use in risk management decisions. The current set of NIST Security Automation specifications includes the Common Vulnerability Scoring System which is a metric-based score for known vulnerabilities in the National Vulnerability Database. This information is used by federal agencies, industry, and internationally as an input to threat metrics for risk based decision making. NIST plans to extend these specifications into additional information areas to further facilitate threat discovery, identification, and measurement.

NIST Cybersecurity Coordination with Other Government Agencies

As mentioned above, NIST is actively engaged with private industry, academia, and other Federal agencies, including those in the NITRD community, in coordination of cybersecurity research and development.

In addition, under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and OMB Circular A-119, NIST is tasked with the key role of encouraging and 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. NIST works with other agencies to coordinate standards issues and priorities with the private sector through consensus standards organizations such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the Institute of Electrical and Electronic Engineers (IEEE), the Internet Engineering Task Force (IETF), the Organization for the Advancement of Structured Information Standards (OASIS), and the International Telecommunication Union (ITU). Key contributions NIST has made include:

- Development of the current Federal cryptographic and cybersecurity assurance standards that have been adopted by many state governments, national governments, and much of industry;
- Development of the identity credentialing and management standard for Federal employees and contractors (also becoming the de facto national standard);
- Development of the standard and conformance test capability for interoperable multi-vendor fingerprint minutia capture and verification;
- Development and demonstration of quantum key distribution;
- Establishment of a national cyber vulnerability database;
- Establishment of U.S. Government IPv6 Test Program;
- Assisting the General Services Administration in deploying DNSSec on the .gov Top Level Domain; and
- Establishment and oversight of an international cryptographic algorithm and module validation program. (Over 1,440 cryptographic module validation certificates have been issued, representing over 3,100 modules. These modules have been developed by more than 335 domestic and international vendors.)

Cybersecurity Legislation

The President made cybersecurity an Administration priority upon taking office. During the release of his *Cyberspace Policy Review* in 2009, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." Over the past two years, the Administration has taken significant steps to ensure that Americans, our businesses, and our government are building better protections against cyber threats. Departments and agencies have implemented programs to enhance their risk management with regard to federal systems.

NIST believes that effective cybersecurity legislation requires an appropriate balance between short and long term goals, as well as providing motivation for strong collaborations between federal agencies, industry, academia, state and local governments and other interested stakeholders. The proposed legislation is focused on improving cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers. NIST looks forward to playing its part, leveraging its legacy of research, development, and standards in this area with other federal and private sector partners.

Conclusion

NIST is actively involved with other federal agencies, industry and academia to address the highest priority cybersecurity research and development needs. NIST's expertise and mission provide the best environment for performing the research necessary to enable the innovative cybersecurity specifications, standards, assurance processes, and training needed for securing U.S. Government and critical infrastructure information systems as well as many other elements of the Nation's digital infrastructure to mitigate the growing threat. Finally, consistent with the NIST 3-Year Planning Report, NIST plans to expand its focus on cybersecurity challenges associated with healthcare IT, the Smart Grid, automation of federal systems security conformance, and cybersecurity game-changing research.

Thank you for the opportunity to testify today on NIST's Federal cybersecurity research and development efforts. I would be happy to answer any questions that you may have.