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

# *"Agency Response to Cyberspace Policy Review"*

June 16, 2009

## Introduction

Chairmen Wu and Lipinski, Ranking Members Smith and Ehlers, and Members of the Subcommittees, I am Cita Furlani, the Director of the Information Technology Laboratory (ITL) 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 cyber security and our perspective on the Administration's 60 Day Cyberspace Policy Review.

As one of the major research components within NIST, our information technology work accelerates the development and deployment of information and communication systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications. NIST accomplishes these goals through collaborative partnerships with our customers and stakeholders in industry, government, academia, and consortia. Based on input from these customers and stakeholders, we have focused our R&D agenda on eight broad program areas: complex systems; cyber and network security; enabling scientific discovery; identity management systems; information discovery, use and sharing; pervasive information technologies; trustworthy information systems; and virtual measurement systems.

Many of our vital programs impact national security, such as improving the accuracy and interoperability of biometrics recognition systems and facilitating communications among first responders. The combination of our mission and legislation such as the Federal Information Security Management Act (FISMA) the Computer Security Research and Development Act, the USA PATRIOT Act, the Enhanced Border Security Act, and the Help America Vote Act lead to rich programmatic diversity.

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 for many years. Through FISMA, Congress again reaffirmed NIST's leadership role in developing standards for cyber security. 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 cyber security 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 recent 60 Day 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 cyber security research, standards development, standards conformance demonstration and cyber security 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 cyber security challenges throughout the information and communications infrastructure through its cross-community engagements. Enabled by Congressional funding increases in 2002 and in response to FISMA legislation, NIST is responsible for establishing and updating, on a recurring basis, the federal government risk management framework and cyber security controls. The national security community, a number of state governments and major private sector organizations are also adopting the risk management framework and cyber security controls designed by NIST. NIST is engaging industry to harmonize product assurance 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 care information technology (HCIT), the Smart Grid, biometrics/face authentication, 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. NIST teams with the Department of Justice and the Small Business Administration in extending cyber security education and training beyond the federal government into the private sector.

Recognizing the importance of security-related standards beyond the federal government, NIST leads national and international consensus standards activities in

cryptography, biometrics, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing.

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), and the International Telecommunication Union (ITU).

Key contributions NIST has made include:

- Development of the current Federal cryptographic and cyber security 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; and
- Establishment and oversight of an international cryptographic algorithm and module validation program. (This Cryptographic Module Validation Program (CMVP) achieved a significant milestone on August 15, 2008, by issuing the program's 1,000th certificate.)

NIST hosts the Information Security Automation Program (ISAP), which formalizes and advances efforts to enable the automation and standardization of technical security operations, including automated vulnerability management and policy compliance evaluations. The NIST National Vulnerability Database (NVD) is the United States Government repository of standards-based vulnerability management reference data. The NVD makes available information on vulnerabilities, impact measurements, detection techniques, and remediation assistance. It provides reference data that enable the ISAP's security automation capabilities. NIST's security automation program is based on the NIST Security Checklist program and the Security Content Automation Protocol (SCAP) activity. The SCAP Validation Program performs conformance testing to ensure that products correctly implement SCAP. NVD also plays a pivotal role in the Payment Card Industry (PCI) in their efforts to mitigate vulnerabilities in credit card systems. The PCI has mandated that

NVD's vulnerability severity scores be used for measuring the risk to payment card servers world-wide and for determining which vulnerabilities must be fixed.

Included in the scope of NIST cyber security activities are the usability of systems such as voting machines and software interfaces; research in mathematical foundations to determine the security of information systems; the National Software Reference Library, computer forensics tool testing, 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 measurement to achieve end-to-end security over heterogeneous, multi-domain networks; biometrics evaluation, usability, and standards (fingerprint, face, iris, voice/speaker, multimodal biometrics) and initiating an international competition for a next generation Secure Hash Algorithm (SHA-3). NIST and the National Science Foundation are co-funding a workshop in July on usability issues associated with security. Among the topics to be investigated are methods to inform individual users of actions they take that could imperil their systems also providing informative justifications, methods and tools to assist administrators of systems in the configuration of their systems to provide secure operation, and forensic tools to help administrators deal with the aftermath of attacks.

Recognizing the value of interagency coordination of research as well as of standards development, NIST actively contributes to the Networking and Information Technology Research and Development (NITRD) program and the development of the NITRD 5-year strategic plan. Within the past year, as provided in the America COMPETES Act (PL 110-69), the NITRD Program has assumed expanded responsibilities for coordination of federal cyber R&D and NIST is well represented in, and leverages, these activities. In addition, NIST collaborates with academia, e.g., individual institutions such as Purdue, and consortia, such as the Institute for Information Infrastructure Protection (or I3P).

NIST works with other members of the Cyber Security and Information Assurance Interagency Working Group in establishing priorities for 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. These systems provide both the basic infrastructure and advanced communications in every sector of the economy, including critical infrastructures such as power grids, emergency communications systems, financial systems, and air-traffic-control networks. These systems also support national defense, national and homeland security, and other vital federal missions, and themselves constitute critical elements of the IT infrastructure. Broad areas of concern which NIST research addresses include Internet and network security; confidentiality, availability, and integrity of information and computer-based systems; new approaches to achieving hardware and software security; testing and

assessment of computer-based systems security; and reconstitution and recovery of computer-based systems and data.

## 60 Day Cyberspace Policy Review

We concur in the findings of the 60 Day Cyber Review relative to the increasingly serious and pervasive threat posed by breaches of - or threats to - our cyber systems, and relative to the need to strengthen the capability of the Executive Office of the President to coordinate the Federal government's response to that threat. We also concur in the report's observation that it is our total national information infrastructure, not just the federal information infrastructure that is faced with the aforementioned threat. We agree that a coordinated response is necessary to prevent catastrophic consequences for those critical infrastructures which integrate information systems into their operations.

While agreeing that it is necessary to integrate the responses of national security organizations and those of federal organizations that do not have a primarily national security mission, we observe that the intelligence community, the other elements of the national security community, and NIST are, in response to the Federal Information Security Management Act of 2002, actively coordinating their standards and processes for cyber security. This effort is producing a single set of requirements, rather than the past's three independent sets of requirements (Intelligence community, national security systems and NIST) for consumers and providers of information processing and interchanges resources.

On June 3rd, NIST announced the release of the final public draft of Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*. The final public draft of Special Publication 800-53, Revision 3, is historic in nature.

For the first time, and as part of the ongoing initiative to develop a unified information security framework for the federal government and its contractors, NIST has included security controls in its catalog for both national security and non national security systems. The updated security control catalog incorporates best practices in information security from the United States Department of Defense, Intelligence Community, and civil agencies, to produce the most broad-based and comprehensive set of safeguards and countermeasures ever developed for information systems.

We are encouraged to observe that the 60 Day Cyberspace Policy Review recognizes that cyber security strategies and solutions must be structured in a manner that accommodates commerce, economic growth, scientific collaboration, and individual liberties. The report reflects the notion that we are not looking for "lockdown solutions" that achieve security at the expense of robust commerce, essential services or civil liberties.

Recognizing the economic impact of cyberspace, NIST is working to provide measurement techniques to facilitate offsetting the cost of both public sector and private sector security solutions by decreases in losses or cost of insurance or increases in business due to increases in trust. Meeting the cyber threat to our national infrastructure would be accelerated by both the public and private sectors if new measurement techniques can demonstrate that increased security is good business sense. We note that not all of these measures need to be technical or regulatory in nature. Some simple, relatively inexpensive, procedural steps can have a materially positive effect on security. One example is the financial sector's having introduced a delay into the conversion of electronically transferred funds into tangible assets, a delay sufficient to permit invocation of fraud detection processes.

We were particularly encouraged by the report's recognition of the role of international standards in protecting our information infrastructure. Our infrastructure is inextricably integrated into a complex of global networks. NIST's role in documentary standards has long been established in law and executive direction. We are actively working with our sister agencies on improving our common understanding of how we can collectively participate, in cooperation with the private sector, in fostering international standards and protocols that are conducive to a free and safe information processing and interchange environment.

NIST and the National Telecommunications and Information Administration (NTIA) are working with the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign on an initiative to enhance the security and stability of the Internet. The parties are working on an interim approach to deployment, by year's end, of a security technology—Domain Name System Security Extensions (DNSSEC)—at the authoritative root zone (i.e., the address book) of the Internet. There will be further consultations with the Internet technical community as the testing and implementation plans are developed. In collaboration with the Department of Homeland Security Science and Technology Directorate, NIST has been an active participant within the international community in developing the DNSSEC protocols and has collaborated with various U.S. agencies in deploying DNSSEC within the .gov domain.

We, at the NIST and the larger Department of Commerce, recognize that we have an essential role to play in realizing the vision set forth in the 60 Day Cyberspace Policy Review. We look forward to working with our federal government partners, with our private sector collaborators, and with our international colleagues to establish a comprehensive set of technical solutions, standards, guidelines, and procedural measures necessary to realizing this vision.

## Conclusion

NIST will continue to conduct the research necessary to enable and to provide cyber security specifications, standards, assurance processes, training and technical expertise needed for securing the U.S. Government and critical infrastructure information systems to mitigate the growing threat. NIST will continue to closely coordinate with domestic and international private sector cyber security programs and national security organizations. Finally, consistent with the NIST 3-Year Planning Report, NIST plans to expand its focus on cyber security challenges associated with healthcare IT, the Smart Grid, automation of federal systems security conformance and status determination, and cyber security leap-ahead research.

Thank you for the opportunity to testify today on NIST's work in the cyber security arena and our views on the President's 60 Day Cyberspace Policy Review. I would be happy to answer any questions you may have.

Cita M. Furlani is Director of the Information Technology Laboratory (ITL). ITL is one of nine research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $85 million, 335 employees, and about 150 guest researchers from industry, universities, and foreign laboratories.

Furlani oversees a research program designed to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics. Through its efforts, ITL seeks to enhance productivity and public safety, facilitate trade, and improve the quality of life.

Furlani has several leadership responsibilities in addition to those at NIST. Currently, she is Co-Chair of the Interagency Working Group on Digital Data, Co-Chair of the Subcommittee on Quantum Information Science, and Co-Chair for Strategic Planning for the Subcommittee on Networking and Information Technology Research and Development, all under the auspices of the National Science and Technology Council. She also serves as Co-Chair of the Technology Infrastructure Subcommittee of the Interagency CIO Council.

Furlani has served as the Chief Information Officer (CIO) for NIST. As CIO, Furlani was the principal adviser to the NIST Director on the planning, execution, evaluation, and delivery of information technology services and support.

Furlani also served as director of the National Coordination Office for Networking and Information Technology Research and Development. This office, reporting to the White House through the Office of Science and Technology Policy and the National Science and Technology Council, coordinates the planning, budget, and assessment activities for the 12-agency Networking and Information Technology R&D Program.

Previously, Furlani was Director of the Information Technology and Electronics Office within the Advanced Technology Program (ATP) at NIST. Before joining ATP, Furlani served as Chief of the Office of Enterprise Integration, ITL, NIST, coordinating Department of Commerce activities in the area of enterprise integration. Furlani also served as special assistant to the NIST Director in the Director's role as Chair of the Committee on Applications and Technology of the Administration's Information Infrastructure Task Force. Previously, Furlani was on detail as technical staff to the Director of NIST in the position of Senior Program Analyst. Prior to August 1992, she managed research and development programs within the NIST Manufacturing Engineering Laboratory, applying information technology to manufacturing since1981.

She earned a Master of Science degree in electronics and computer engineering from George Mason University and a Bachelor of Arts degree in physics and mathematics from Texas Christian University. She was awarded two Department of Commerce Bronze Medal Awards in 1985 and 1993 and the Department of Commerce Silver Medal Award, in 1995.