

Testimony of

Cita M. Furlani  
Director

Information Technology Laboratory

National Institute of Standards and Technology  
United States Department of Commerce

United States House of Representatives  
Committee on Science and Technology  
Subcommittee on Technology and Innovation

“Cybersecurity Activities at NIST’s Information  
Technology Laboratory”

October 22, 2009

Chairman Wu, Ranking Member Smith, and Members of the Subcommittee, 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 cybersecurity and our perspective on the Administration's Cyberspace Policy Review Recommendations.

As one of the major research components within NIST, the Information Technology Laboratory accelerates the development and deployment of information and communication systems that are reliable, usable, interoperable, and secure; advance measurement science through innovations in mathematics, statistics, and computer science; and develop the measurements and standards infrastructure for emerging information technologies and applications. In addition to research into cybersecurity technologies, NIST is responsible for development of, publishing, and providing explanatory support for Federal cybersecurity standards, guidelines, and best practices. Just as the standards function extends beyond writing Federal standards to playing an active role in the development of national and international consensus standards, the support function is extended to state and local governments and private sector elements that voluntarily adopt NIST-developed cybersecurity standards.

NIST doesn't rely solely on Federal resources and insights. We employ collaborative partnerships with our customers and stakeholders in industry, government, academia, and consortia to take advantages of their technical and operational insights and to leverage the resources of a global community. We are actively seeking to expand the scope of these collaborative efforts in general, and of our private sector collaborations in particular.

The impacts of NIST's cybersecurity activities extend beyond providing the means to protect Federal IT systems. They provide the cybersecurity foundations for the public trust that is essential to our realizing the national and global productivity and innovation potential of electronic business and its attendant economic benefits.

The cybersecurity standards and support capabilities of NIST's Information Technology Laboratory rest on the foundation of the laboratory's cybersecurity research and development activities. Based on input from our 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 in ways that extend beyond what are generally recognized as the boundaries of cybersecurity. Examples of these impacts include improving the accuracy and interoperability of biometrics recognition systems and facilitating communications among first responders. The combination of our mission and legislative mandates such as the Federal Information Security Management Act

(FISMA), the Cyber 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.

Cybersecurity is a vital, central mission of our laboratory. 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 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.

The Cyberspace Policy Review observes that it is our total national information infrastructure, not just the federal information infrastructure, which is under attack, recognizing a national response is necessary to prevent catastrophic consequences for society, including those critical infrastructures which integrate information systems into their operations. To provide for such a national response, the President has developed a coordinated approach that places leadership for cybersecurity-related policies within the White House. This includes the appointment of a Chief Technology Officer, located in the Office of Science and Technology Policy, a Chief Information Officer in the Office of Management and Budget, and the pending appointment of a Cyber Advisor in the White House. This team provides an effective means for coordination and collaboration across the Federal government and with the private sector. This includes integrating the responses of national security organizations and those of federal organizations that do not have a primarily national security mission. In fact, 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 cybersecurity. This effort is producing a single set of requirements, rather than the past's three independent sets of requirements for consumers and providers of information processing and interchanges resources.

A key output of this initiative to develop a unified information security framework for the federal government and its contractors occurred on August 1, 2009, when NIST announced the release of Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*. NIST Special Publication 800-53, Revision 3, is historic in nature. For the first time, NIST has included security controls in its catalog for both national security and nonnational 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. This unified framework provides a standardized method for expressing security at all levels, from operational implementation to compliance reporting. This allows for an environment of information sharing and interconnections among these communities and significantly reduces costs, time, and resources needed for finite sets of systems and administrators to report on cybersecurity to multiple authorities.

The NIST Identity Management Systems Program is pursuing the development of critical standards and metrics to support the effective management of digital identities for large-scale enterprises throughout their life cycle. These efforts will improve the strength, usability, and interoperability of identity management systems; protect users' personal data; and assure that U.S. interests on this issue are represented in the international arena. We have been heavily involved in federal government identity management efforts, including developing the standard for the personal identity verification (PIV) card in response to HSPD-12 and co-chairing the National Science and Technology Council (NSTC) Identity Management Task Force.

The Cyberspace Policy Review included in its top ten action items, "Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation." To this end, NIST is working with the Office of Science and Technology Policy, the Office of Management and Budget (OMB), and the National Security Council staff to determine how to address this action item, through a new Sub-Interagency Policy Committee which will focus on online identity management.

NIST is taking other proactive steps to increase the long-term security of federal information systems. Working with the Office of Management and Budget and several federal agencies, NIST is helping to develop a Security and Privacy Profile that will provide guidance to enterprise architects on integrating information security and privacy requirements into the Federal Enterprise Architecture. This initiative will ensure that information security and privacy requirements are built into federal information systems early in the system development life cycle rather than attempting to add these requirements after systems are deployed into operational environments. NIST will also be working with its partners within the federal government to publish guidance on best practices in systems and security engineering to address the effective integration of commercial information technology products into federal information systems. This guidance will build on the excellent work published by the National Security Agency as part of the Information Assurance Technical Framework over a decade ago and make the information widely available to both public and private sector entities.

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), which is funded by the National Cybersecurity Division of the Department of Homeland Security, 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 worldwide and for determining which vulnerabilities must be fixed.

In addition to the initiatives described above, NIST has implemented an aggressive outreach program to work with state, local, and tribal governments as well as private sector entities to raise the awareness of government officials and corporate executives with regard to the ongoing and increasingly sophisticated nature of cyber threats. The outreach program will help organizations external to the federal government have a better understanding of NIST's suite of security standards and guidelines and provide an opportunity for voluntary adoption of the standards and guidelines by those organizations to facilitate an increased level of information security for the nation's critical information infrastructure.

On a broader scale, in response to the Cyberspace Policy Review's recommendation to initiate a national public awareness and education campaign to promote cybersecurity and as a contribution to October's Cyber Security Awareness Month, NIST, working with the Small Business Administration and the Federal Bureau of Investigation, has published a guide to help small businesses and organizations understand how to provide basic security for their information, systems, and networks. The 20-page guide, *Small Business Information Security: The Fundamentals*, uses simple and clear language to walk small business owners through the important steps necessary to secure their computer systems and data. The guide provides ten "absolutely necessary steps" to secure information, which includes such basics as installing firewalls, patching operating systems and applications, and backing up business data, as well as controlling physical access to network components and training employees in basic security principles. NIST also created a video that explores the reasons small businesses need to secure their data.

We are encouraged to observe that the Cyberspace Policy Review recognizes that cybersecurity 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 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. In order to meet the cyber threat to our total national infrastructure, we must demonstrate that implementing measures that increase security is good business sense. We'd note that not all of these measures need to be technical or regulatory in nature. Some simple 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.

As acknowledged in the Cyberspace Policy Review, measurement of information security performance can benefit organizations in many ways, by increasing accountability, improving the effectiveness of safeguards, demonstrating legislative and policy compliance, and providing quantifiable inputs for risk-based resource allocation decisions. The Cyberspace Policy Review recommended strengthening federal leadership and accountability for cybersecurity, including identifying cybersecurity as a management priority and assessing the progress of federal agencies against cybersecurity goals, ultimately leading to increased accountability, compliance with cybersecurity policies, and effective implementation of cybersecurity safeguards. Because of its strengths in measurement science and cybersecurity, NIST was asked by OMB to contribute to the Security Metrics Taskforce. This taskforce was established to develop new outcome-focused, rather than compliance-focused, metrics for information security performance for federal agencies, resulting in more effective provisioning of security controls and resources, and improved protection in support of critical mission and business 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, including the Department of State, 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.

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 such as the State Department 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 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; 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.)

Understanding 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 Five-year strategic plan. Within the past year, the NITRD Program has assumed expanded responsibilities for coordination of federal cyber research and development, and NIST is well represented in, and leverages, these activities.

The Cyberspace Policy Review challenged the federal networks and Information Technology (IT) research community to develop a framework for research and development strategies that focus on game-changing technologies. Over the past year, through the National Cyber Leap Year and a wide range of other activities, the government research community, including NIST, sought to elicit the best game-changing ideas from the broader research and technology community.

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.

There are others ways in which NIST's expertise can help to drive improvements in the cybersecurity arena. NIST has integral roles in a number of Administration initiatives, including Health Information Technology, Smart Grid, Broadband, and Web 2.0. NIST can continue to work on more effective metrics (security controls effectiveness determination), expand education and other outreach, improve product assurance processes, expand national and international cybersecurity standards participation, and automate security controls. This is in addition to our cryptography, technical guidelines, and best practices work.

To address the interdisciplinary nature of security in cyberspace, ITL also has programs in the usability of systems such as voting machines, health information technology 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 supervisory control and data acquisition 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; and biometrics evaluation, usability, and standards (fingerprint, face, iris, voice/speaker, multimodal biometrics.) Research activities in ITL 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.

We, at NIST and the Department of Commerce, recognize that we have an essential role to play in realizing the vision set forth in the Cyberspace Policy Review. NIST will continue to conduct the research necessary to enable and to provide cybersecurity 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 cybersecurity programs and national security organizations. Finally, consistent with the NIST Three-Year Planning Report, NIST plans to broaden its focus on cybersecurity challenges associated with health IT, the Smart Grid, automation of federal systems security conformance and status determination, and cybersecurity leap-ahead research.

Cybersecurity is a vital, central mission of our laboratory. Given the increasing importance and complexity of cybersecurity, NIST has undertaken an internal assessment of its operational structure and allocation of resources to ensure that ITL programs fully reflect the complex interdisciplinary nature of today's threats. For example, NIST is considering whether it needs to strengthen the authority and purview of the NIST Chief Cybersecurity Advisor. Regardless of whatever recommendations emerge from this internal assessment, the technical program of work currently performed by the Computer Security Division would not change. NIST welcomes, through our Advisory Committee, key external stakeholders, and this Subcommittee, input on NIST operations and structure and looks forward to continued conversations on this matter.

Thank you for the opportunity to testify today on NIST's work in the cybersecurity arena. I would be happy to answer any questions you may have.