**Testimony of**

**Patrick D. Gallagher, Ph.D.**
**Under Secretary of Commerce for**
**Standards and Technology**
**United States Department of Commerce**

**Before the**
**United States Senate**
**Committee on Appropriations**

# "Cybersecurity: Preparing for and Responding to the Enduring Threat"

**June 12, 2013**

**Introduction**
Chairwoman Mikulski, Vice-Chairman Shelby, members of the Committee, I am Patrick Gallagher, Under Secretary of Commerce for Standards and Technology and Director of the National Institute of Standards and Technology (NIST), a non-regulatory bureau within the U.S. Department of Commerce. I am also currently serving as the Acting Deputy Secretary of Commerce. Thank you for this opportunity to testify today on NIST's roles and responsibility for cybersecurity.

**The Role of NIST in Cybersecurity**
NIST's overall mission is 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. Our work in addressing technical challenges related to national priorities has ranged from projects related to the Smart Grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, when it was given the responsibility for the development of the Data Encryption Standard. Our role 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, was then strengthened through the Computer Security Act of 1987 and reaffirmed through the Federal Information Security Management Act of 2002.

Consistent with our mission, NIST actively engages with industry, academia, and other parts of the Federal government including the intelligence community, and with elements of the law enforcement and national security communities. These collaborations inform our efforts in coordinating and prioritizing cybersecurity research, standards development, standards conformance demonstration and cybersecurity education and outreach.

Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users, from small and medium enterprises to large private and public organizations including agencies of the Federal government and companies involved with critical infrastructure.

We employ collaborative partnerships with our customers and stakeholders in industry, government and academia, 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 Initiative for Cybersecurity Education (NICE), National Strategy for Trusted Identities in Cyberspace (NSTIC), the National Cybersecurity Center of Excellence (NCCoE), and through development of the Cybersecurity Framework under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."

My testimony has four parts today: I'll discuss the role of NIST in protecting Federal information systems; our engagement with industry; our work under the President's Executive Order; and how our funding supports all of those efforts.

**The Role of NIST in Protecting Federal Information Systems**

The E-Government Act of 2002, Public Law 107-347, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, known as the Federal Information Security Management Act of 2002 (FISMA), included duties and responsibilities for the National Institute of Standards and Technology to develop standards and guidelines for Federal information systems.

The NIST Special Publications (SPs) and Interagency Reports (IRs) provide management, operational, and technical security guidelines for Federal agencies and cover a broad range of topics such as BIOS management and measurement, key management and derivation, media sanitization, electronic authentication, security automation, Bluetooth and wireless protocols, incident handling and intrusion detection, malware, cloud computing, public key infrastructure, risk assessments, supply chain risk management, authentication, access control, security automation and continuous monitoring.

Beyond these documents - which are peer-reviewed throughout industry, government, and academia - NIST conducts workshops, awareness briefings, and outreach to ensure comprehension of standards and guidelines, to share ongoing and planned activities, and to aid in scoping guidelines in a collaborative, open, and transparent manner.

In support of FISMA implementation, in recent years NIST has strengthened its collaboration with the Department of Defense, the Intelligence Community, and the Committee on National Security Systems, through the Joint Task Force Transformation Initiative, which continues to develop key cybersecurity guidelines for protecting Federal information and information systems for the Unified Information Security Framework.

This collaboration allows 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. It 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.

To support agency implementation of cloud technology, NIST has worked with the General Services Administration (GSA) to help establish the Federal Risk and Authorization Management Program (FedRAMP) to identify security assessment requirements, and prototype a process for approving Third-Party Assessment Organizations (3PAOs) that demonstrate capability in assessing Cloud Service Provider (CSP) information systems for conformance to identified standards and guidelines.

Given DHS's important role in Federal agency cybersecurity, our partnership with DHS informs NIST's collaborative efforts. Earlier in the year I signed a Memorandum of Agreement with DHS Undersecretary Rand Beers to ensure that our work with industry on cybersecurity standards, best practices, and metrics, is fully integrated with the information sharing, threat analysis, response, and other work of DHS. We believe this will help enable a more holistic approach to addressing the complex nature of the challenge facing Federal agencies.

**NIST's Engagement with Industry**

It is important to note that the impact of NIST's activities under FISMA 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. Many organizations voluntarily follow these standards and guidelines, reflecting their wide acceptance throughout the world.

Beyond our responsibilities under FISMA, under the provisions of the National Technology Transfer and Advancement Act, Public Law 104-113, and related 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).

A partnership with industry to develop, maintain, and implement voluntary consensus standards related to cybersecurity best practices promotes the interoperability, security and resiliency of this global infrastructure and makes 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.

NIST also conducts cybersecurity research and development in areas such as security for federal mobile environments and techniques for measuring and managing security. These efforts focus on improving the cybersecurity of current and future information technologies, and on improving the trustworthiness of IT components such as claimed identities, data, hardware, and software for networks and devices.

In addition, NIST recognizes that further development of cybersecurity standards will be needed to improve the security and resiliency of critical U.S. information and communication infrastructure. The availability of cybersecurity standards and associated

conformity assessment schemes is essential to these efforts, which will help enhance the deployment of sound security solutions and build trust among those creating and those using the solutions throughout the country.

Additionally, the state of Maryland, Montgomery County, and NIST have jointly established the National Cybersecurity Center of Excellence (NCCoE), a public-private collaboration for accelerating the widespread adoption of cybersecurity technologies. Through the creation of standards-based reference designs, templates, and example "builds," the NCCoE will reduce barriers for companies that see the deployment of more secure technologies as too costly, too complicated, or technically infeasible. Reducing these economic, educational, and technical barriers to adoption can improve the security posture, and increase the competitiveness, of U.S. industry.

The NCCoE tackles some of the most pressing cybersecurity challenges identified by the members of one or more economic sectors. These challenges are then synthesized into specific "use cases" that include technical details that allow the NCCoE to develop an integrated solution based on commercially available technology. All of this work is done in an open and collaborative process: the use cases are published for public comment on the NCCoE website; the solutions are developed in collaboration with the private sector, other government agencies, and academia; the NCCoE hosts workshops and public meetings to exchange expertise and validate the practicality of the solutions under development; and, when complete, the entire set of material necessary to recreate the NCCoE example solution is made available to the public.

The NCCoE is a unique opportunity that brings together, under one roof, experts from industry, government, and academia to develop practical, interoperable, and usable cybersecurity solutions. The center collaborates with the private sector primarily through three channels:

- A sector community of interest, open to the public, with primary participation drawn from sector-specific businesses (e.g., Healthcare, Financial Services, Energy, etc.).
- National Cybersecurity Excellence Partnership companies –U.S. IT and cybersecurity companies that have committed to share technology and engineering staff with the NCCoE on persistent basis.
- Use case collaborators –companies that are providing a secure technology and engineering expertise as a part of an integrated solution for a specific use case.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is another key area in which NIST engages with industry. Under NSTIC, NIST is working with a wide array of stakeholders on creation of an online environment—the "Identity Ecosystem"—that addresses the myriad security and convenience problems caused by passwords, and allows individuals and organizations to better trust one another, with minimized disclosure of personal information. The Identity Ecosystem will be a user-centric online environment, supported by a framework of technologies, policies, and agreed-upon

standards, which will enable individuals to transact business in a way that is more secure, convenient and privacy-enhancing everywhere they go online.

In the Identity Ecosystem, consumers will be able to choose in the marketplace from a variety of identity solutions — both private and public — that would issue trusted credentials that could be used in lieu of passwords across the Internet. Key attributes of the Identity Ecosystem include privacy, convenience, efficiency, ease-of-use, security, confidence, innovation, and choice. Creating this Identity Ecosystem requires a partnership between the private sector, advocacy groups, public sector agencies and others – all of whom are currently working to support NSTIC by collaborating in the privately led Identity Ecosystem Steering Group (IDESG). The request continues and expands existing efforts to coordinate federal activities needed to implement NSTIC.

NIST also supports the continued work under the National Initiative for Cybersecurity Education (NICE). As we all know, cybersecurity is much more than technological solutions to technical problems; it is also highly dependent on educated users who are aware of and routinely employ sound practices when dealing with cyberspace. NIST will continue to work with the Federal government, and with state, local, and tribal governments, for improving cybersecurity education. NIST will ensure coordination, cooperation, focus, public engagement, technology transfer, and sustainability of NICE. NIST works with DHS and other Federal agencies in the implementation of the cybersecurity education framework to address national cybersecurity awareness, formal cybersecurity education, Federal cybersecurity workforce structure, and cybersecurity workforce training and professional development.

Small businesses face particular cybersecurity challenges, as they tend to have more limited resources that must be well applied to meet the most obvious and serious threats. The vulnerability of any individual small business may not seem significant, other than to the owner and employees of that business. However, given that over 95 percent of all U.S. businesses are small- and medium-size businesses (SMBs), a vulnerability common to a large percentage of SMBs poses a threat to the Nation's economic base. SMBs frequently cannot justify an extensive security program or a full-time expert. Nonetheless, they confront serious security challenges and must address security requirements based on identified needs.

Cognizant of the needs of SMBs, NIST partners with the Small Business Administration (SBA) and the Federal Bureau of Investigation’s InfraGard program to sponsor computer security workshops and provide online support for small businesses. Through these efforts, experts in computer security are made available to offer small business owners an overview of information security threats, vulnerabilities, and corresponding protective tools and techniques, with a special emphasis on providing useful information that small business personnel can apply directly or use to task contractor personnel.

In FY12, NIST, SBA, and the FBI hosted 25 small business information security workshops in Oklahoma, Louisiana, Colorado, New Hampshire, Connecticut, Minnesota,

Texas, California, Indiana, Ohio, and New Mexico, and provided online support to SMBs throughout the United States.

**NIST's role in Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"**

As you know, on February 13, 2013, the President signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which gave NIST the responsibility to develop a framework to reduce cyber risks to critical infrastructure (the Cybersecurity Framework). As directed in the Executive Order, NIST, working with industry, will develop the Cybersecurity Framework and the Department of Homeland Security (DHS) will establish performance goals. DHS, in coordination with sector-specific agencies, will then support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities, through a voluntary program. NIST is also working closely with partners throughout the interagency – including the intelligence community – to ensure that the Framework leverages their expertise and role as the Framework is developed.

A Cybersecurity Framework is an important element in addressing the challenges of improving the cybersecurity of our critical infrastructure. A NIST-coordinated and industry-led Framework will draw on standards and best practices that industry already develops and uses. NIST coordination will ensure that the process is open and transparent to all stakeholders, and will ensure a robust technical underpinning to the framework. This approach will significantly bolster the relevance of the resulting Framework to industry, making it more appealing for industry to adopt.

This multi-stakeholder approach leverages the respective strengths of the public and private sectors, and helps develop solutions in which both sides will be invested. The approach does not dictate solutions to industry, but rather facilitates industry coming together to offer and develop solutions that the private sector is best positioned to embrace. Any efforts to better protect critical infrastructure need to be supported and implemented by the owners and operators of this infrastructure.

Underlying all of this work, NIST sees its role in developing the Cybersecurity Framework as partnering with industry and other stakeholders to help them develop the Framework. In addition to this critical convening role, our work will be to compile and provide guidance on principles that are applicable across the sectors for the full-range of quickly evolving threats, based on inputs from DHS and other agencies. NIST's unique technical expertise in various aspects of cybersecurity related research, technology development and an established track record of working with a broad cross-section of industry and government agencies in the development of standards and best practices positions us very well to address this significant national challenge in a timely and effective manner.

NIST's initial steps towards implementing the Executive Order included issuing a Request for Information (RFI) in February to gather relevant input from industry and other stakeholders, and asking stakeholders to participate in the Cybersecurity

Framework process. NIST is following up the RFI process with continued engagement with stakeholders through a series of workshops and events to ensure that we can cover the breadth of considerations that will be needed to make this national priority a success. We have already initiated an aggressive outreach program to raise awareness of this issue and begin engaging industry and stakeholders. NIST will continue bring many diverse stakeholders to the table. Last week, a 3-day workshop hosted by Carnegie Mellon University in Pittsburgh allowed NIST to engage with stakeholders to discuss the foundations of the Framework and the initial analysis.

The Executive Order requirement for the Framework to be developed within one year, and a preliminary framework due within eight months gives this task a sense of urgency. Throughout the year, you can expect NIST to use its capabilities to gather the input needed to develop the Framework.

In a year's time, once we have developed an initial Framework, we will continue to need to work with DHS, sector-specific agencies, and the specific sectors themselves to build strong voluntary programs for specific critical infrastructure areas. Their work will then inform the needs of critical infrastructure and the next versions of the Framework. The goal at the end of this process will be for industry to take and manage the Cybersecurity Framework – allowing it to evolve when needed.

Although this Executive Order will help raise the nation's cyber defenses, it does not eliminate the urgent need for legislation in these and other areas of cybersecurity. The Administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account two years of public and congressional discourse about how best to improve the nation's cybersecurity.

The Administration is working toward legislation that:

- Facilitates cybersecurity information sharing between the government and the private sector as well as among private sector companies. We believe that such sharing can occur in ways that protect privacy and civil liberties protections, reinforce the appropriate roles of civilian and intelligence agencies, and include targeted liability protections.

- Incentivizes the adoption of best practices and standards for critical infrastructure by complementing the process set forth under the Executive Order;

- Gives law enforcement the tools to fight crime in the digital age;

- Updates Federal agency network security laws, and codifies DHS' cybersecurity responsibilities; and

- Creates a National Data Breach Reporting requirement.

In each of these legislative areas, the right privacy and civil liberties safeguards must be incorporated. The Administration wants to continue the dialogue with the Congress and stands ready to work with members of Congress to incorporate our core priorities to produce cybersecurity information sharing legislation that addresses these critical issues.

**NIST Support for Cyber R&D**

As highlighted today Cybersecurity is a top priority for NIST, which has been reflected in our recent budget requests. In FY2013 NIST has proposed to increase cybersecurity spending by $7.5M with most of this increase supporting NIST's efforts to develop a framework to reduce cyber risks to critical infrastructure in support of the EO. In the President's FY 2014 budget request NIST has requested a $24M dollar increase to its cybersecurity R&D programs for a total NIST investment in cybersecurity and related efforts of $68M. The requested increases for NIST in FY2014 will provide additional support for NIST's roles in cyber education, identity management, and will support R&D to improve the security and interoperability of our nation's cyberspace infrastructure, accelerate the development and adoption of cybersecurity standards in support of Administration priorities, and to support the leading-edge work of the National Cybersecurity Center of Excellence (NCCoE).

**Conclusion**

The cybersecurity challenge facing critical infrastructure – both in the "dot gov" and the "dot com" is greater than it ever has been. Active collaboration within the public sector, and between the public and private sectors, is the only way to effectively meet this challenge, leveraging both sectors' roles, responsibilities, and capabilities.

Thank you for the opportunity to present NIST's views regarding cybersecurity security challenges. I appreciate the Committee holding this hearing. I look forward to working with the Committee to help address these pressing challenges. I will be pleased to answer any questions you may have.

## Patrick D. Gallagher

Dr. Patrick Gallagher was confirmed as the 14th Director of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) on Nov. 5, 2009. He also serves as Under Secretary of Commerce for Standards and Technology, a new position created in the America COMPETES Reauthorization Act of 2010, signed by President Obama on Jan. 4, 2011.

Gallagher provides high-level oversight and direction for NIST. The agency promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. NIST's FY 2012 resources total $750.8 million from the Consolidated and Further Continuing Appropriations Act of 2012 (P.L. 112-55), with an estimated additional annual income of $62.7 million in service fees, and $128.9 million from other agencies. The agency employs about 2,900 scientists, engineers, technicians, support staff, and administrative personnel at two main locations in Gaithersburg, Md., and Boulder, Colo.

Gallagher had served as Deputy Director since 2008. Prior to that, he served for four years as Director of the NIST Center for Neutron Research (NCNR), a national user facility for neutron scattering on the NIST Gaithersburg campus. The NCNR provides a broad range of neutron diffraction and spectroscopy capability with thermal and cold neutron beams and is presently the nation's most used facility of this type. Gallagher received his Ph.D. in Physics at the University of Pittsburgh in 1991. His research interests include neutron and X-ray instrumentation and studies of soft condensed matter systems such as liquids, polymers, and gels. In 2000, Gallagher was a NIST agency representative at the National Science and Technology Council (NSTC). He has been active in the area of U.S. policy for scientific user facilities and was chair of the Interagency Working Group on neutron and light source facilities under the Office of Science and Technology Policy. Currently, he serves as co-chair of the Standards Subcommittee under the White House National Science and Technology Council.