Testimony of

Dr. Patrick Gallagher
Under Secretary of Commerce
for Standards and Technology
and
Director, National Institute of Standards and Technology
United States Department of Commerce

Before the
United States Senate
Committee on Commerce, Science, and Transportation

"The Partnership between NIST and the Private Sector: Improving Cybersecurity"

July 25, 2013

Introduction
Chairman Rockefeller, Ranking Member Thune, members of the Committee, I am Pat Gallagher, Director of the National Institute of Standards and Technology (NIST), a non-regulatory bureau within the U.S. Department of Commerce. Thank you for this opportunity to testify today on NIST's role under the President's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" and NIST's responsibility to develop a framework to reduce cyber risks to critical infrastructure. I want to acknowledge and thank this Committee for its leadership and support on this issue.

The Role of NIST in Cybersecurity
NIST's 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, we have worked with federal agencies, industry, and academia since 1972 starting with 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 strengthened through the Computer Security Act of 1987 and reaffirmed through the Federal Information Security Management Act of 2002.

Consistent with this mission, NIST actively engages with industry, academia, and other parts of the Federal government including the intelligence community, and elements of the law enforcement and national security communities, 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 federal government agencies and companies involved with critical infrastructure.

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"
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). The Executive Order directed NIST to work with industry and develop the Cybersecurity Framework and the Department of Homeland Security (DHS) will establish performance goals. DHS, in collaboration with sector-specific agencies, will support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities through a voluntary program.

Our partnership with DHS drives much of our effort. Earlier this year, we signed a Memorandum of Agreement with DHS to ensure that our work on the Cybersecurity Framework and the development of cybersecurity standards, best practices, and metrics, is fully integrated with the information sharing, threat analysis, response, and operational work of DHS. We believe this will enable a more holistic approach to address the complex challenges we face.

A Cybersecurity Framework is an important element to address the challenges of improving the cybersecurity of our critical infrastructure. A NISTcoordinated and industry-led Framework will draw on standards and best practices that industry already develops and uses. NIST ensures that the process is open and transparent to all stakeholders including industry, state and local government and academia, and ensures a robust technical underpinning to the Framework. This approach will significantly bolster the Cybersecurity Framework to industry.

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. It also ensures the framework is flexible enough to be applicable to small and mid-sized entities.

I would also like to note that this is not a new or novel approach for NIST. We have utilized similar approaches in the recent past to address other pressing national priorities. For example, NIST's work in the area of Cloud Computing technologies enabled us to develop important definitions and architectures, and is now enabling broad federal government deployment of secure Cloud Computing technologies. The lessons learned from this experience and others inform how we plan for and structure our current effort.

Developing the Cybersecurity Framework

The Cybersecurity Framework will consist of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks for critical infrastructure. Regulatory agencies will also review the Cybersecurity Framework to determine if current cybersecurity requirements are sufficient, and propose new actions to ensure consistency. Independent regulators are also encouraged to do the same.

This approach reflects both the need for enhancing the security of our critical infrastructure and the reality that the bulk of critical infrastructure is owned and operated by the private sector. Any efforts to better protect critical infrastructure must be supported and implemented by the owners and operators of this infrastructure. It also reflects the reality that many in the private sector are already doing the right things to protect their systems and should not be diverted from those efforts through new requirements.

Current Status of the Cybersecurity Framework and Partnering with Industry
NIST sees its role in developing the Cybersecurity Framework as partnering with industry and other stakeholders to help them develop the Framework. NIST's unique technical expertise in various aspects of cybersecurity related research and technology development, and our 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) this past February to gather relevant input from industry and other stakeholders, and asking stakeholders to participate in the Cybersecurity Framework process. Given the diversity of sectors in critical infrastructure, the initial efforts are designed to help identify existing cross-sector security standards and guidelines that are applicable to critical infrastructure.

A total of 244 responses were posted on NIST's website. Responses ranged from individuals to large corporations and trade associations and also included comments as brief as a few sentences on specific topics, as well as so comprehensive that they ran over a hundred pages. We published an analysis of these comments in May.

NIST is also engaging 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. Our first such session – held in April – initiated the process of identifying existing resources and gaps, and prioritized the issues to be addressed as part of the Framework.

At the end of May, a second workshop at Carnegie Mellon University brought together a broad cross-section of participants representing critical infrastructure owners and operators, industry associations, standards developing organizations, individual companies, and government agencies. This three-day working session, using the analysis of the RFI comments as input, was designed to identify and achieve consensus on the standards, guidelines, and practices that will be used in the Framework.

Based on the responses to the RFI, conclusions from the workshops, and NIST analyses, the preliminary Framework is designed and intended:

- To be an adaptable, flexible, and scalable tool for voluntary use;
- To assist in assessing, measuring, evaluating, and improving an organization's readiness to deal with cybersecurity risks;
- To be actionable across an organization;
- To be prioritized, flexible, scalable, performance-based, and cost-effective;
- To rely on standards, guidelines and practices that align with policy, business, and technological approaches to cybersecurity;
- To complement rather than to conflict with current regulatory authorities;

- To promote, rather than to constrain, technological innovation in this dynamic arena;
- To focus on outcomes;
- To raise awareness and appreciation for the challenges of cybersecurity but also the means for understanding and managing the related risks;
- To protect individual privacy and civil liberties; and
- To be built upon national and international standards and other standards, best practices and guidelines that are used globally.

Last week, NIST held its third workshop to present initial considerations for the Framework. This workshop had a particular emphasis on issues that have been identified from the initial work – including the specific needs of different sectors. During the workshop, NIST gained consensus on the elements of the Framework that include:

- A section for senior executives and others on using this Framework to evaluate an organization's preparation for potential cybersecurity-related impacts on their assets and on the organization's ability to deliver products and services. By using this Framework, senior executives can manage cybersecurity risks within their enterprise's business plans and operations.
- A User's Guide to help organizations understand how to apply the Framework.
- Core Sections to address:
    - Five major cybersecurity functions and their categories, subcategories, and informative references;
    - Three Framework Implementation Levels associated with an organization's cybersecurity functions and how well that organization implements the Framework; and
    - A compendium of informative references, existing standards, guidelines, and practices to assist with specific implementation.

At eight months, we will have a preliminary Framework that builds on these elements. In a year's time, once we have developed an initial Framework, there will still be much to do. For example, we will work with specific sectors 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 itself to take "ownership" and update the Cybersecurity Framework.

Conclusion

The cybersecurity challenge facing critical infrastructure is greater than it ever has been. The President's Executive Order reflects this reality, and lays out an ambitious agenda focused on collaboration between the public and private sectors. NIST is mindful of the weighty responsibilities with which we have been charged by President Obama, and we are committed to listening to, and working actively with, critical infrastructure owners and operators to develop a Cybersecurity Framework.

The approach to the Cybersecurity Framework set out in the Executive Order will allow industry to protect our Nation from the growing cybersecurity threat while enhancing

America's ability to innovate and compete in a global market. It also helps grow the market for secure, interoperable, innovative products to be used by consumers anywhere.

Thank you for the opportunity to present NIST's views regarding critical infrastructure cybersecurity security challenges. I appreciate the Committee holding this hearing. We have a lot of work ahead of us, and I look forward to working with this Committee and others to help us 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. Prior to his appointment as NIST Director, Gallagher had served as Deputy Director since 2008.

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 2013 budget includes $778.0 million in direct and transfer appropriations, an estimated $49.7 million in service fees and $120.6 million from other agencies. The agency employs about 3,000 scientists, engineers, technicians, support staff, and administrative personnel at two main locations in Gaithersburg, Md., and Boulder, Colo. NIST also hosts about 2,700 associates from academia, industry, and other government agencies, who collaborate with NIST staff and access user facilities. In addition, NIST partners with more than 1,300 manufacturing specialists and staff at more than 400 MEP service locations around the country.

Under Gallagher, NIST has greatly expanded its participation, often in a leadership role, in collaborative efforts between government and the private sector to address major technical challenges facing the nation. NIST’s participation in these efforts stems from the agency’s long history of technical accomplishments and leadership in private-sector led standards-development organizations and in research fields such as manufacturing engineering, cybersecurity and computer science, forensic science, and building and fire science. Currently, he co-chairs the Standards Subcommittee under the White House National Science and Technology Council.

Gallagher joined NIST in 1993 as a research physicist and instrument scientist at the NIST Center for Neutron Research (NCNR), a national user facility for neutron scattering on the NIST Gaithersburg campus. In 2000, he became group leader for facility operations, and in 2004 he was appointed NCNR Director. In 2006, the U.S. Department of Commerce awarded Gallagher a Gold Medal, its highest honor, for his leadership in interagency coordination efforts.

Gallagher received his Ph.D. in physics at the University of Pittsburgh and a bachelor’s degree in physics and philosophy from Benedictine College.