Testimony of

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

Before the
United States House of Representatives

Committee on Energy and Commerce

"Cyber Threats and Security Solutions"

May 21, 2013

Introduction
Chairman Upton, Ranking Member Waxman, 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. Thank you for this opportunity to testify today on NIST's role under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" and our responsibility to develop a framework for reducing cyber risks to critical infrastructure.

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 on 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 agencies of the federal government 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). 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.

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.

I would also like to note that this is not a new or novel approach for NIST. We have utilized very similar approaches in the recent past to address other pressing national priorities. The lessons learned from those experiences are informing how we are planning for and structuring our current effort. In 2007, the Energy Independence and Security Act (EISA) mandated NIST to develop a standards framework to help with the deployment of a nationwide, end-to-end interoperable Smart Grid. Following a similar approach to the one envisioned for the Cybersecurity Framework, NIST coordinated a forward leaning approach involving more than 1500 representatives from approximately 21 distinct domains that now constitute the Smart Grid.

This effort led to the development of a framework called the Smart Grid Roadmap that defined the domains of the Smart Grid and the interfaces for those domains, identified existing standards for these domains, prioritized standards needs and identified standards gaps. Many of these standards gaps are currently being addressed in various standards development organizations around the world. We are seeing the results of this effort pay off in many ways. Cybersecurity standards are being developed and adopted to secure different elements of the electrical grid. Standards based deployments of secure Smart Meters are enabling consumers safe and secure access to data about electricity usage. The U.S. Smart Grid Roadmap is being used as a template for frameworks in many countries around the world. Automakers are reaching agreement regarding chargers for electric vehicles. All these developments have helped address important policy objectives while also positioning the U.S. as a leader in Smart Grid development and deployment.

Another example of how NIST has brought together the public and private sector to address technical challenges is NIST's work in the area of Cloud Computing technologies. The unique partnership formed by NIST has enabled us to develop important definitions and architectures, and is now enabling broad federal government deployment of secure Cloud Computing technologies.

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. Once the Framework is established, the Department of Homeland Security (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. Regulatory agencies will also review the Cybersecurity Framework to determine if current cybersecurity requirements are sufficient, and propose new actions to ensure consistency.

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 need to 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.

The Important Role of Standards in the Cybersecurity Framework

I'd like to explain why this approach relies on standards, methodologies, procedures and processes, and why we believe it to be a critical part of our work under the Executive Order. First of all, by standards, I am referring to agreed-upon best practices against which we can benchmark performance. Thus, these are NOT regulations. Typically these standards are the result of industry coming together to develop solutions for market needs and are developed in open discussions and agreed upon by consensus of the participants.

This process also gives standards the power of broad acceptance around the world. Standards have a unique and key attribute of scalability. By this I mean, that when we can use solutions that are already adopted by industry, or can readily be adopted and used by industry, then those same solutions reduce transactions costs for our businesses and provide economies of scale when deployed in other markets, which makes our industries more competitive.

A partnership with industry to develop, maintain, and implement voluntary consensus standards related to cybersecurity best ensures 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.

Current Status of the Cybersecurity Framework

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 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 help identify existing cross-sector security standards and guidelines that are immediately applicable or likely to be applicable to critical infrastructure.

The responses to the RFI – a total of 244 – were posted on NIST's website. Those responding ranged from individuals to large corporations and trade associations, and they provided comments as brief as a few sentences on specific topics, as well as so comprehensive that they ran to over 100 pages. NIST is currently conducting an analysis of these comments, with our initial observations shared publicly just last week.

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. Next week at a workshop hosted by Carnegie Mellon University in Pittsburgh, we will again be working with stakeholders to discuss the foundations of the Framework and the initial analysis.

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.

Next Steps

The Executive Order requirement for the Framework to be developed within one year, with a preliminary Framework due within eight months, highlights this task's urgency. 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 through a series of "deep-dive" engagements. Throughout the year, you can expect NIST to use its capabilities to gather the input needed to develop the Framework.

Next month, the Departments of Commerce, Homeland Security, and Treasury will submit reports regarding incentives designed to increase participation in the voluntary program. NIST will be supporting the report drafted by the Department of Commerce, which will analyze the benefits and relative effectiveness of such incentives.

In July NIST will host its third workshop to present initial considerations for the Framework, based on the analysis conducted of the responses to the RFI. This workshop will be the most in-depth of the four, with an emphasis on particular issues that have been

identified from the initial work – including the specific needs of different sectors. At eight months, we will have an initial draft Framework that clearly outlines areas of focus and initial lists of standards, guidelines and best practices that fall into those areas

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– ensuring that the Framework will continue to evolve as needed.

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 founded on active 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.

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, 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.