Testimony of

Charles H. Romine
Director, Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives

Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

"Oversight of Executive Order 13636 and Development of the Cybersecurity Framework"

July 18, 2013

Introduction
Chairman Meehan, Ranking Member Clarke, members of the Subcommittee, I am Chuck Romine, Director of the Information Technology Laboratory 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 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 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.

Our partnership with DHS will drive 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 also with 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 addressing the complex challenges we face.

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 is ensuring 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. 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 are informing how we are planning for and structuring 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. Once the final 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.

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. 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 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, repeatable, 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 be built upon 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 organizations ability to deliver products and services. By using this Framework, senior executives can manage cybersecurity risks within their enterprise's broader risks and 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.
    - 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– 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.

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.

Charles H. Romine

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $120 million, more than 350 employees, and about 160 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program designed to promote U.S. innovation and industrial competitiveness by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for Federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission 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.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

Education:

Ph.D. in Applied Mathematics from the University of Virginia

B.A. in Mathematics from the University of Virginia.