Testimony of

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

United States Senate

Committee on Commerce, Science and Transportation

"Building a More Secure Cyber Future: Examining Private Sector Experience with the NIST Framework"

February 4, 2015

Introduction

Chairman Thune, Ranking Member Nelson and Members of the Committee, I am Dr. Charles Romine, 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 NIST's work in cybersecurity.

The Role of NIST in Cybersecurity

With programs focused on national priorities from the Smart Grid and electronic health records to forensics, atomic clocks, advanced nanomaterials, and computer chips and more, 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 the quality of life.

In the area of cybersecurity, NIST has worked with Federal agencies, industry, and academia since 1972, starting with the development of the Data Encryption Standard, when the potential commercial benefit of this technology became clear. NIST's role, to research, develop and deploy information security standards and technology to protect the Federal government's information systems against threats to the confidentiality, integrity and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. § 3541[1]) and recently reaffirmed in the Federal Information Security Modernization Act of 2014 (Public Law 113-283). Importantly, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure – consistent with NIST's role in implementation of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity".

NIST accomplishes its mission in cybersecurity through collaborative partnerships with its customers and stakeholders in industry, government, academia, standards bodies, consortia and international partners.

NIST Engagement with Industry

Beyond NIST's responsibilities under FISMA, under the provisions of the National Technology Transfer and Advancement Act (PL 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.

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347; 116 Stat. 2899).

NIST works with other agencies, such as the Department of State, 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 Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunications Union (ITU).

Partnership with industry to develop, maintain, and implement voluntary consensus standards related to cybersecurity best ensures the interoperability, security and resiliency of the global infrastructure needed to make 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 believes 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 in these efforts, which NIST supports to help enhance the deployment of sound security solutions and build trust among those creating and those using the solutions throughout the country.

Cybersecurity Framework: Current Status

Almost one year ago, NIST issued The Framework for Improving Critical Infrastructure Cybersecurity *(*Framework) in accordance with Section 7 of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (Executive Order). The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

Executive Order 13636 was designed to increase protection across the full range of Critical Infrastructure – those systems and assets that the Nation's economic and national security rely upon. Under Executive Order 13636, Federal government security agencies were charged to increase the flow of valuable threat information to industry, and NIST was charged to play a convener and facilitator role in supporting the private sector's efforts to develop the Cybersecurity Framework.

The goal of the Framework is to help organizations align their policies, technologies, and day-to-day business operations to better protect their data and their information technology (IT) and industrial control systems.

The Framework also was designed to assess the capacity of the market to deliver better cybersecurity protection. During the development process for the Framework, NIST asked industry to contribute ideas about what standards, guidelines, and best practices could be used more widely to better manage cybersecurity risks, and then

what steps should be taken to develop the next set of tools in these public-private partnerships.

In the course of developing the Framework document published in February of 2014, NIST estimates that more than 3,000 people from industry, academia, and government came to participate in workshops and webinars, while providing hundreds of detailed comments on drafts. The NIST approach was premised on the understanding that a Framework designed by industry would gain greater adoption throughout the private sector, and could support a vibrant market for IT security products and services.

The result of this effort is a dynamic tool that has two main parts.

First, the Framework is a collection of existing standards and best practices that proved to be helpful in protecting systems from cyber threats and ensuring business confidentiality, while protecting individual privacy and civil liberties.

Second, the Framework sets out basic guidelines that organizations can use in adopting those practices, providing them with a coherent structure to consider the many, varied approaches to cybersecurity that have proliferated in recent years.

NIST heard over and over that a key challenge facing information security professionals, senior business leaders, and company executives and boards of directors striving to address cybersecurity, was the lack of a common vocabulary and approach. As a result, the Framework starts with general guidance, and cascades to the more technical and specific, to help facilitate that dialogue with and within an organization.

The fact that the Framework is – and will remain – voluntary has allowed NIST to continue to bring the maximum number of stakeholders to the table. And the inherent flexibility of the Framework allows each organization to tailor it to individual needs.

Since the release of the Framework, NIST has strengthened its collaboration with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders to raise awareness about the Framework, encourage use by organizations across and supporting the critical infrastructure, and develop implementation guides and resources.

NIST, along with its partners across government, has focused on building on that initial awareness and on working arm-in-arm with the private sector as the Framework begins to be used within organizations, and as those organizations develop supporting products and services.

The Framework was designed to be a “living” document, shaped by the experiences of those using it. To learn more about these experiences, NIST released a Request

for Information (RFI)[2] on August 26, 2014, and held its 6th Cybersecurity Framework Workshop at the University of South Florida in Tampa, Florida, on October 29 and 30, 2014. Responses to the RFI came from industry, academia and government organizations at multiple levels, as well as organizations representing large constituencies and key stakeholders in critical infrastructure sectors.

Based on that feedback, and NIST's continued work, I'd like to share some thoughts about where NIST is now - almost a year since the release of the Framework.

NIST found that organizations are using the Framework in a variety of ways. Many users have found the Framework helpful in raising awareness and communicating with stakeholders within their organization, including executive leadership. It is also being used to improve communications across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors. The Framework is being used to demonstrate alignment with standards, guidelines, and best practices. The Framework is also being used as a strategic planning tool to assess risks and current practices.

In addition to those "users," we have been encouraged by seeing expanding networks -- within and across sectors of the economy – beginning to learn about and take advantage of the Framework, making it more relevant to their stakeholders.

This includes:

- Technology companies have been developing products and services aligned with the Framework.

- Communities of interest and associations have been sharing practical advice to help organizations to optimize their use of the Framework.

- The auditing community has begun to leverage the Framework to provide a consistent auditable standard.

- Major insurance providers have begun to offer policies tied to the Framework and are promoting it among their policy-holders.

- States have begun to leverage the Framework to improve the security of their infrastructure, including as a foundation for their work in cybersecurity for state emergency management agencies.

And, in part because the Framework incorporates globally recognized voluntary standards for cybersecurity, it is serving as a model for other countries, allowing them to match their business' perspectives with their governments' needs. In other words, this is not a "U.S.-only" Framework.

---

[2] RFI - Experience with the Framework for Improving Critical Infrastructure Cybersecurity, August 26, 2014, https://federalregister.gov/a/2014-20315

Cybersecurity Framework: Next Steps

NIST is continuing its outreach and awareness program through discussions with international partners, global companies and other interested governments, while NIST continues the primary outreach efforts to U.S. industries and organizations. This includes outreach to regulatory agencies, to facilitate a consistent understanding of the Framework across the Federal government, and to reinforce that the Framework is not designed or intended to create additional requirements for owners and operators of critical infrastructure, who are otherwise subject to regulatory requirements.

As NIST learns from individual organizations about their experiences with the Framework – good or otherwise – NIST hopes to share that knowledge and insight with others so that they may gain confidence in using the Framework. NIST also hopes to provide specifics, for example, through appropriate "case studies," for those who are seeking more information on how to build or improve their own cybersecurity programs.

The data that is collected and reflected will be the source information for any determinations or suggestions for changes that might be needed to the Framework going forward. The Framework is envisioned as a "living document." At this point, however, there is rather widespread agreement among workshop participants that it is too soon to consider updating the Framework, and that NIST should continue efforts to promote understanding and use of the current version. This will allow industry the time to implement, for tools and service to be built and offered, as well as for the common vocabulary of the Framework to become established. In any event, any changes that might be made to the Framework will be made through the same open, transparent and inclusive process that was used in the initial creation of the Framework.

In the months ahead, NIST will focus on the challenging aspects of implementation and will consider producing guidance that will help organizations address these challenges. No modifications or new versions of the Framework are anticipated within the next year, although NIST will continue to work on areas singled out in the *Roadmap for Improving Critical Infrastructure Cybersecurity,*[3] released the same time as the Framework. NIST also will continue to explore options for future governance of the Framework, based on NIST's appreciation of the long-term benefits of the Framework becoming a private-sector maintained process in the future.

NIST will continue, and increase, its efforts to raise awareness of the Framework, including through partnerships with other organizations. NIST's efforts will be carried out in the same open and collaborative manner which was the hallmark of the Framework's development. One priority will be to develop and disseminate information and training materials that advance use of the Framework, such as actual or exemplary illustrations of how organizations of varying sizes, types, and

[3] http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf

cybersecurity capabilities can practically employ the Framework to make themselves more secure.

National Initiative for Cybersecurity Education

I would like to provide you now with an update on NIST's work to support building a capable cybersecurity workforce – a workforce that is agile and can adapt to meet the national need to design, develop, implement, maintain and continuously improve cybersecurity, consistent with the relevant provisions of the Cybersecurity Enhancement Act of 2014.

In 2010, the National Initiative for Cybersecurity Education (NICE) was established to enhance the overall cybersecurity posture of the United States by accelerating the availability of educational, training, and workforce development resources designed to improve the cybersecurity behavior, skills, and knowledge of every segment of the population. As the lead agency for this initiative, NIST works with more than 20 Federal departments and agencies, as well as with industry and academia, to raise national awareness about risks in cyberspace, broaden the pool of individuals prepared to enter the cybersecurity profession, and cultivate a globally competitive cybersecurity workforce.

NICE has also aligned with the President's Job-Driven Training Initiative to increase the number of individuals who complete high-quality cybersecurity training and education programs and attain the skills most needed to provide a pipeline of skilled workers for industry and government.

Additional Research Areas

NIST performs research and development in related technologies, such as the usability of systems including electronic health records, voting machines, biometrics and software interfaces. NIST is performing basic research on the mathematical foundations needed to determine the security of information systems. In the areas of digital forensics, NIST is enabling improvements in forensic analysis through the National Software Reference Library and computer forensics tool testing. Software assurance metrics, tools, and evaluations developed at NIST are being implemented by industry to help strengthen software against hackers. NIST responds to government and market requirements for biometric standards by collaborating with other Federal agencies, academia, and industry partners to develop and implement biometrics evaluations, enable usability, and develop standards (fingerprint, face, iris, voice/speaker, and multimodal biometrics). NIST plays a central role in defining and advancing standards, and collaborating with customers and stakeholders to identify and reach consensus on cloud computing standards.

Conclusion

NIST recognizes that it has been entrusted with an essential role in helping industry, consumers and government to manage cybersecurity risks.

NIST is extremely committed to fulfilling that role; it is committed to improving on existing cybersecurity technical solutions, standards, guidelines, and best practices, through robust collaborations with our Federal government partners, private sector collaborators, and international colleagues; and NIST is committed to helping to ensure that government needs stay aligned with, and are informed by, the needs of American industry.

But let us be clear, and here I am not telling this Committee anything it does not know well: even with the body of work that is now behind us, there is still much to do. NIST will continue a sustained dialogue between government and the private sector to ensure it can be responsive to ever-evolving cybersecurity challenges, and in this NIST has appreciated the support of the Committee.

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

Charles H. Romine

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of seven research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of $150 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.