Testimony of

Donna F. Dodson
Chief Cybersecurity Advisor
National Institute of Standards and Technology
United States Department of Commerce

Before the United States Senate

Committee on Homeland Security and Governmental Affairs

"*Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure*"

March 26, 2014

Introduction

Chairman Carper, Ranking Member Coburn and Members of the Committee, I am Donna F. Dodson, the Chief Cybersecurity Advisor working in the Information Technology Laboratory (ITL) in the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for this opportunity to testify today on NIST's responsibilities under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" and our work through public-private partnerships in the area of cybersecurity.

Background

Let me begin with a few words on NIST itself: 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 in the smart grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips.

In cybersecurity, we have worked with federal agencies, industry, and academia dating back to the mid-1970s 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. Consistent with this mission, NIST actively engages with private industry, academia, non-national security federal departments and agencies, the intelligence community, and other elements of the law enforcement and national security communities.

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 critical infrastructure companies.

The Role of NIST in Executive Order 13636

NIST has spent the last year working to convene Critical Infrastructure sectors to build a Cybersecurity Framework as part of Executive Order 13636. Version 1.0 of the Framework was released on February 12, 2014, along with a Roadmap for future NIST work in support of this effort.

The Executive Order asked NIST to develop a Framework – a collection of industry standards, process, and best practices – that could be leveraged more broadly to help companies manage their cybersecurity risk. NIST's approach was to work with stakeholders to develop a structure that any organization, large or small, in any one of the varied critical infrastructure sectors can use to begin, or make improvements to, their current cybersecurity programs. The Framework offers a common language to address and manage cyber risks in a cost-effective way based on business needs without placing additional compliance obligations on businesses.

We found that the voluntary nature of the Framework has encouraged the widest set of stakeholders to come to the table and work collaboratively. This approach, with its reliance on voluntary standards, is already consistent with U.S. policy and business use because they have proven to work. Time and time again, when industries get together and determine for themselves what standards describe a quality product, those standards are much more likely to be adopted quickly and to be fully implemented.

I would like to make one other key point. The Framework was designed with the nation's critical infrastructure in mind. But it also can be used by any organization, regardless of its role in society. The broader the effective use of the Framework and its underlying capabilities, the greater the likelihood that our Nation's infrastructure will be secure.

Framework Development Process

Going back to the title of the hearing, I would like to talk about the public-private partnership that the Administration used to develop the Framework. NIST began the process with a Request for Information and received hundreds of submissions from stakeholders in industry, academia, and government. Those submissions, which we posted publicly, provided a foundation for the Framework. But it was only a start; supporting and building on that initial dialogue, we held five workshops around the country with thousands of participants, providing draft versions of the Framework and supporting material multiple times on our website, encouraging comments on all of the material, and carefully considering all the feedback we received.

Organizations across the critical infrastructure, large and small, in many sectors, academia and government were consulted and involved from start to finish. Much of that engagement included international organizations and even other countries. This is a good thing: by having international scale it can be further embraced by the market, creating a suite of truly interoperable products that can be leveraged by anyone.

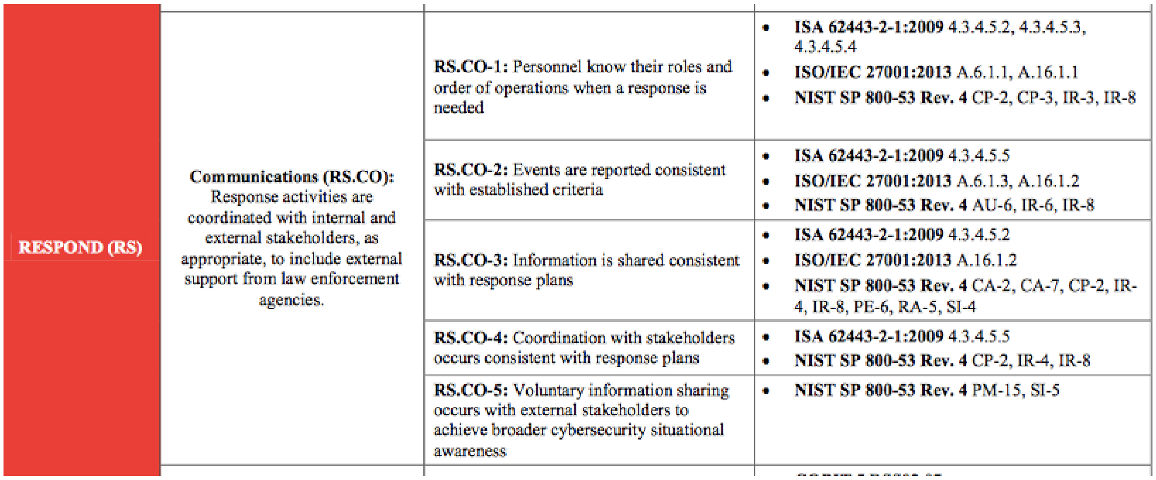
The Framework

The result of this effort is a document that lays out the critical elements of any cybersecurity program and then links those elements to proven standards and protections for organizations to consider using.

This approach reinforces key processes that all organizations consider as they balance risk to be effective. Through this view, it allows senior leadership's engagement in the cybersecurity risk management process, provides a mechanism to provide accountability and responsibility, and tools for the fusion of threat and vulnerability information with potential impact to business needs and operational capabilities.

The Framework consists of three parts: the Framework Core, the Framework Profiles, and the Framework Tiers.

The Framework Core consists of five Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. While they do not replace a risk management process, these five high-level Functions can also help an organization answer fundamental questions, including "How are we doing?" Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary. The Framework Core also provides additional detail, all the way down to the technical implementation as reflected in standards and guidelines, on how a security program can be created. An example from the "Respond" function is below.



RESPOND (RS)	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• **NIST SP 800-53 Rev. 4** PM-15, SI-5

Figure 1: Example from the Framework Core

Framework Implementation Tiers then provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. During the Tier selection process, an organization will consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. These Tiers reflect a progression from informal, reactive implementations to approaches that are agile and threat-informed.

A Framework Profile represents the outcomes that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Most importantly, profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the desired state). Organizations can use that information to develop action plans to strengthen existing cybersecurity practices and reduce cybersecurity risk. Organizations may also find that they are overinvesting to achieve certain outcomes and can reprioritize resources to strengthen other cybersecurity practices.

As part of the ongoing work, we believe that organizations will draft sample profiles to illustrate sector-specific needs and requirements – including regulatory and legal obligations.

It is also important to note that the Framework offers guidance regarding privacy and civil liberties considerations that may result from cybersecurity operations. While processes and existing requirements will differ, the Framework can assist organizations in considering privacy and civil liberties as part of a comprehensive cybersecurity program – highlighting risks to privacy and civil liberties that can emerge when developing such a program and helping to mitigate them.

Together we think this structure will enable organizations to improve their practices. By mapping their individual cybersecurity programs against the full list of cybersecurity functions, categories, and specific standards, companies can identify gaps and tailor improvement plans to their specific needs. They can then create internal metrics to track and document those improvements. Some companies may discover in the process that their entire cybersecurity effort consists only of passwords and antivirus software with no real-time detection capability even though automated tools are widely available and affordable. Other companies may find the Framework a useful tool for holding their suppliers accountable or for purchasing these services in a more systematic way.

The bottom line is that we believe the Framework can provide an agreed-upon way to talk clearly to one another about cybersecurity issues and solutions. This in turn, we believe will help us make great strides in strengthening the security and resilience of Critical Infrastructure from cyberthreats.

Next Steps for the Framework

While today's Framework is the culmination of a year-long effort that brought together thousands of individuals and organizations from industry, academia and government, it is just another step in a continuous process to improve the Nation's cybersecurity. The Framework is a living document that will need to be updated to keep pace with changes in technology, threats and other factors, and to incorporate lessons learned from its use. These updates will ensure the Framework meets the needs of critical infrastructure owners and operators in a dynamic and challenging environment.

Today, many organizations, led by their senior executives, are using the Framework and providing feedback to NIST and the Department of Homeland Security. This will help us identify improvements needed in the Framework. Industry groups, associations, and non-profits are playing key roles in assisting their members to understand and use the Framework. They are building or mapping their sector's specific standards, guidelines and best practices to the Framework. They are developing and sharing examples of how organizations are using the Framework.

In developing the Framework we also understood that many issues would require additional work with our stakeholders before they could be included in the Framework. These issues became a Roadmap to accompany the Framework that we released on February 12th. This companion Roadmap for the Framework captures NIST's future directions and plans for the Framework and identifies the most important areas for development, alignment, and collaboration. In the near-term, NIST will continue to serve as a convener and coordinator to work with industry and other government agencies to help organizations understand, use and improve the Framework. But we will also hold discussions of models for future governance of the Framework, such as potential transfer to a non-government organization. Like the Framework itself, these plans are based on input and feedback received from the private sector as well as other government agencies. The Roadmap lays out a path toward an improved Framework and a fully developed and functioning ecosystem to support voluntary use of – and improvements to – that document.

The Cybersecurity Framework and its accompanying Roadmap represent a piece of a continuing conversation about how to better protect those critical assets. We look forward to continuing to work collaboratively with industry and government to lower cybersecurity risks and better protect our economy and national security.

Other NIST Public–Private Partnerships in Cybersecurity

NIST's strong partnerships with industry, academia, and government are vital to the success of all our cybersecurity programs in cybersecurity. This reflects our traditional role in innovative research leading to the development of standards and best practices for Federal Departments and Agencies, as well as new programs, notably the National Strategy for Trusted Identities in Cyberspace (NSTIC) and the National Cybersecurity Center of Excellence (NCCoE).

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

The NIST Special Publications (SPs) and Interagency Reports provide those management, operational, and technical security guidelines for Federal agencies and cover a broad range of topics such as BIOS management and measurement, cryptography, key management, security automation, Bluetooth and wireless protocols, incident handling and intrusion detection, malware, cloud computing, public key infrastructure, risk assessments, usability, 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.

It is important to note that the impact of NIST's activities under FISMA extend beyond providing the means to protect Federal information technology 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. As we further learned in the Framework development process, many organizations voluntarily follow these standards and guidelines, a reflection of their wide acceptance throughout the world.

Beyond the 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. 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 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.

In addition, further development of underlying 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 builds trust among those creating and those using the solutions throughout the country.

National Strategy for Trusted Identities in Cyberspace

NIST also houses the National Program Office established to lead implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC). NSTIC is an initiative that aims to address one of the most commonly exploited vectors of attack in cyberspace: the inadequacy of passwords for authentication.

Poor authentication mechanisms are a commonly exploited vector of attack by adversaries. The 2013 Data Breach Investigations Report (conducted by Verizon in concert with the U.S. Department of Homeland Security) noted that in 2012, 76% of network intrusions exploited weak or stolen credentials. In line with the results of this report, Target has revealed that this was the vector taken by its attacker, with a compromised credential of one of its business partners being used to access its network.

NSTIC aims to address this issue by collaborating with the private sector to catalyze a marketplace of better identity and authentication solutions – an "Identity Ecosystem" that raises the level of trust associated with the identities of individuals, organizations, networks, services, and devices online. NIST has funded a dozen pilots and supported work in the privately-led Identity Ecosystem Steering Group (IDESG) to craft standards to improve authentication online.

National Cybersecurity Center of Excellence

In 2012, The National Cybersecurity Center of Excellence (NCCoE) was formed as a partnership between NIST, the State of Maryland, and Montgomery County to accelerate the adoption of security technologies that are based on standards and best practices. The center is a vehicle for NIST to work directly with businesses across various industry sectors on applied solutions to intractable cybersecurity challenges. Today the NCCoE has programs working with the healthcare, financial services, and energy sectors in addition to addressing challenges that cut across sectors including: mobile device security, software asset management, cloud security, and identity management. We are also working to show how these technologies can assist in the implementation of the Cybersecurity Framework.

Conclusion

We at the NIST, and our colleagues within the Department of Commerce, recognize that the cybersecurity challenge facing this Nation is greater than it has ever been. We are committed to listening to the private sector and to working as part of the private-public sector team to address this challenge. In particular, NIST will continue to support a comprehensive set of technical solutions, standards, guidelines, and best practices that are necessary to address this challenge.

Thank you for the opportunity to testify today on NIST's work to develop and advance the use of the *Framework for Improving Critical Infrastructure Cybersecurity* and related activities. I would be happy to answer any questions you may have.

Donna Dodson
Chief Cybersecurity Advisor, Information Technology Laboratory, NIST

Donna Dodson is also the Division Chief of the Computer Security Division (CSD) and the Acting Executive Director of the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST). Donna oversees the CSD cybersecurity research program to develop standards, guidelines, technology, tests and metrics for the protection of unclassified Federal information and systems. Through partnerships with industry, Dodson also ensures NIST cybersecurity contributions help secure the Nation's sensitive information and systems. This includes establishing public-private collaborations for accelerating the widespread adoption of integrated cybersecurity tools and technologies.

Dodson received one Department of Commerce Gold Medal and three NIST Bronze Medals. She was a recipient of a 2011 Federal 100 Award for her contributions to advancements in cybersecurity and included in the Top 10 Influential People in Government Information Security.