Testimony of

Charles H. Romine, Ph.D.

Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Research and Technology

“Strengthening U.S. Cybersecurity Capabilities”

February 14, 2017

Introduction

Chairwoman Comstock, Mrs. Johnson, and members of the Subcommittee, 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 key roles in cybersecurity. Specifically, today I will discuss NIST's activities that help strengthen the Nation's cybersecurity capabilities.

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, 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 our 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 reaffirmed in the Federal Information Security Modernization Act of 2014 (Public Law 113-283). In addition, 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.

Cybersecurity Commission

The Commission on Enhancing National Cybersecurity was established by Executive Order 13718 in February of last year, as a limited-duration, independent, bipartisan advisory committee within the Department of Commerce. The stated goals for the Commission were to enhance cybersecurity awareness and protections at all levels of government, business, and society; to protect privacy, to ensure public safety and economic and national security; and to empower Americans to take better control of their digital security. The Executive Order charged the Commission to produce and to publish a final report, after which it would be terminated.

On December 2, 2016, the Commission released its report, which provides detailed short- and long-term recommendations to strengthen cybersecurity in both the public and private sectors, while protecting privacy, fostering innovation and ensuring

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

economic and national security. NIST provided support to the commissioners as they consulted technical and policy experts, solicited input from the public through open hearings and a request for information, reviewed existing literature, and technical input during development of the final report.

The report emphasizes the need for collaborations between the public and private sectors, as well as international engagement. It also discusses the role consumers must play in enhancing our digital security. The report categorizes its recommendations within six overarching imperatives:

- Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks;
- Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy;
- Prepare Consumers to Thrive in a Digital Age;
- Build Cybersecurity Workforce Capabilities;
- Better Equip Government to Function Effectively and Securely in the Digital Age; and
- Ensure an Open, Fair, Competitive, and Secure Global Digital Economy.

NIST is active in several of these imperatives, which are addressed below.

Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks

Cybersecurity Framework

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

Since the release of the Framework, NIST has strengthened its collaborations 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.

Last month, NIST released a draft update to the Framework incorporating feedback received since the release of Framework version 1.0, comments from a December 2015 Request for Information, and from a 2016 Cybersecurity Framework Workshop. Draft Version 1.1 of the Framework, for which NIST is seeking public comments through April 10 of this year, provides new details on managing supply chain risks, clarifies key terms,

and introduces measurement methods for cybersecurity. Key to the continuing success of the Framework is that it is not regulatory or mandatory in nature, but rather, is voluntarily implemented by industry and voluntarily adopted by infrastructure sectors, contributing to reducing cyber-risks to our Nation's critical infrastructure.

Cybersecurity for the Internet of Things

NIST works with stakeholders across industry, academia, and organizations that develop international standards and governments to cultivate trust in the Internet of Things (IoT). NIST performs fundamental research, contributes to the development of consensus standards, and issues guidance that address security for IoT in areas such as: Lightweight Encryption; RFID (Radio-Frequency Identification) and Bluetooth Security; BIOS Integrity; Industrial Control Systems Security; Blockchain; and Verifiable Time. NIST's applied research for IoT security addresses market-focused applications such as Health Information Technology, Vehicle/Transportation, Smart Home, and Manufacturing. For example, NIST's National Cybersecurity Center of Excellence (NCCoE) engineers are working with the healthcare community to address wireless infusion pump security in hospital environments. NIST is also working with the smart home industry to explore authentication and privacy preserving data sharing of IoT devices in a home environment and with the automotive industry toward integration of security, safety, resilience, reliability, and privacy in connected vehicle design and testing.There are many other NIST projects that cross-cut with IoT research, such as the Cybersecurity Framework, the National Vulnerability Database (already extended to include IoT devices and known IoT vulnerabilities), Supply Chain Risk Management for Information and Communication Technology, and guidance on systems security engineering (NIST Special Publication 800-160).

Authentication and Identity Management

Identity and access management processes are key elements of many of the cybersecurity technologies identified above, and are necessary to the effective specification and application of these technologies to counter cyber-threats. Authentication of people, information, and system components underlies the selection, application, and management of cybersecurity technical, procedural and management controls.

NIST develops best practices to support user digital identities, building on decades of research in technology areas that support authentication and identity management. Recently, NIST published for comment a major revision to NIST Special Publication 800-63, now titled *Digital Identity Guidelines*. The guidelines cover remote authentication of users (such as employees or contractors) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, and related assertions.

NIST is working to accelerate adoption of identity and access management technologies that expand the use of digital Personal Identity Verification credentials to

mobile devices and private sector organizations. One example includes implementation of a centralized system to authenticate and control individuals' access to IT and operational resources of electrical generation and distribution systems. NIST is also researching requirements for standards and best practices for digital device identity for IoT devices and working with industry to support implementation of those standards and recommendations.

Privacy

NIST provides guidance and tools for organizations to address privacy risk by designing privacy into their systems from the beginning. Last month, NIST released Internal Report (NIST IR) 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*. NIST collaborated with stakeholders in the public and private sectors, academia, and civil society organizations to develop a foundational framework to support privacy engineering and risk management. The report also provides a platform for integrating privacy into NIST's cybersecurity activities and programs, including the Cybersecurity Framework, Internet of Things, identity management, and the NCCoE. Aligned with the NIST mission, protecting privacy is good for innovation and U.S. competiveness in the digital economy, improving our quality of life.

Build Cybersecurity Workforce Capabilities

National Initiative for Cybersecurity Education

As the cybersecurity threat and technology environment evolves, the cybersecurity workforce must continue to adapt to design, develop, implement, maintain, and continuously improve upon current cybersecurity practices, including in our Nation's critical infrastructure.

In 2008, the National Initiative for Cybersecurity Education (NICE), a public-private collaboration among government, academia, and industry, was established to enhance the overall cybersecurity capabilities of the U.S. The NICE program seeks to energize and promote a robust ecosystem for cybersecurity education, training, and workforce development. 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 ensure a digital economy enabled by a knowledgeable and skilled cybersecurity workforce.

In November 2016, NIST released the draft *NICE Cybersecurity Workforce Framework*, to help our Nation more effectively identify, recruit, develop, and maintain its cybersecurity talent. The framework provides a common language to categorize and describe cybersecurity work that will help organizations build a strong labor staff to protect systems and data. The NICE Challenge Project, funded by NIST and developed and maintained by California State University, San Bernardino, creates virtual challenges to test students and professionals on their ability to perform NICE Framework tasks and exhibit their knowledge, skills, and abilities.

In 2016, CyberSeek, an interactive online tool designed to help close the cybersecurity skills gap, was released to the public. CyberSeek, developed by CompTIA and Burning Glass, with funding from NIST, provides detailed, actionable data about supply and demand in the cybersecurity job market. CyberSeek includes an interactive map that indicates relative concentrations of cybersecurity job postings and worker supply. The Career Pathway portal of CyberSeek provides information on different types of cybersecurity positions to help students, job seekers, and education and training providers. The Career Pathway portal features information on common job titles, salaries, in-demand skills, education and certifications related to careers in cybersecurity, as well as pathways to reaching the mid- to advanced-level career positions.

NIST is also piloting the establishment of Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development in five communities[2] across the U.S. The RAMPS work to bring together K-12 schools, community colleges, universities, training providers, economic development organizations, local and state government, and employers to coordinate regional activities addressing the cybersecurity workforce shortage and expand their local economy.

Better Equip Government to Function Effectively and Securely in the Digital Age

Enterprise Risk Management

NIST carries out its responsibilities under both the Federal Information Security Management and Modernization Acts (FISMA) through the creation of a series of Federal Information Processing Standards (FIPS) and associated guidelines and practices. Under these laws, federal agencies are required to implement NIST's FIPS. NIST provides management, operational, and technical security guidelines for federal agencies covering a broad range of topics, such as protecting the confidentiality of Controlled Unclassified Information while residing in nonfederal information systems and organizations, BIOS management and measurement, key management and derivation, media sanitization, electronic authentication, and security automation.

NIST has a series of specific responsibilities with respect to federal agency information and information systems, other than National Security Systems, under both the Federal Information Security Management Act of 2002 and the Federal Information Security Modernization Act of 2014, including the development of:

- A standard for categorizing information to be used by all federal agencies. The categories are based on the potential impact of harm to the organization if the information or information systems are compromised; and

[2] Albany, New York; the Virginia Tidewater region; the Cincinnati-Dayton Corridor of Ohio; Colorado Springs, Colorado; and Phoenix, Arizona

- Minimum security requirements (*i.e.*, management, operational, and technical controls), for each information category.

In support of FISMA implementation, in recent years NIST has strengthened its collaboration with the Department of Defense, the Intelligence Community, and the Committee on National Security Systems, through the Joint Task Force Transformation Initiative, which continues to develop key cybersecurity guidelines for protecting federal information and information systems.

This collaboration allows for a broad-based and comprehensive set of safeguards and countermeasures for information systems. This unified framework provides a standardized method for expressing security at all levels, from operational implementation to compliance reporting. It allows for an environment of information-sharing and interconnections among these communities and significantly reduces costs, time, and resources needed for finite sets of systems and administrators to report on cybersecurity to multiple authorities.

NIST provides standards, guidelines, and tools for agencies to test and assess their security and then to continuously monitor their implementation and new risks. This process is essential to ensure security baselines are initially implemented correctly, and remains pertinent even as technologies, threats, and missions continuously evolve.

Under FISMA, NIST does not assess, audit, or test agency security implementations and has no oversight authority. Congress recognized that placing such responsibilities on NIST would impede and ultimately defeat its ability to work with federal agency and private sector stakeholders to develop standards, guidelines, and practices in the open, transparent, and collaborative manner Congress intended.

Accordingly, compliance and oversight authority resides with other agencies, such as the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). Federal agency heads, in coordination with their Chief Information Officers and Senior Agency Information Security Officers, report the security status of their information systems to OMB in accordance with annual FISMA reporting guidance. In addition, agency Inspectors General provide an independent assessment of the security status of federal information systems, also reporting results to OMB annually.

NIST's statutory role as the developer—but not the enforcer—of standards and guidelines under FISMA has ensured NIST's ongoing ability to engage freely and positively with federal agencies on the implementation challenges and issues they experience in using these standards and guidelines. NIST meets frequently with agencies and holds regular Federal Security Manager Forums to discuss these issues, our standards and guidance, share lessons learned, and gain insights into methods and means to continually improve our standards, guidelines, and practices.

NIST is actively considering additional steps to assist federal agency cybersecurity practices, including ways in which Federal agencies might take advantage of the

voluntary Cybersecurity Framework in implementing NIST's FISMA suite of standards, guidelines and best practices. Thoughtful application of the risk-based approach of the Cybersecurity Framework across the federal government could complement and enhance agency efforts to implement their programs. NIST will continue to seek to minimize the burden placed upon implementing departments and agencies by building from existing evaluation and reporting regimes, and encouraging common and comparable evaluation of cybersecurity capabilities across federal departments and agencies, given the diversity of missions, requirements and risk environments.

The President signed the American Innovation and Competitiveness Act (Public Law 114-329), which passed both Houses of the 114th Congress with bipartisan support, and amended the NIST Organic Act to include new requirements for research and analysis on the information security and challenges faced by the Federal government. NIST looks forward to working with this Congress and its stakeholders in government and industry on implementing these important provisions.

Conclusion

NIST recognizes that it has an essential role to play in helping industry, consumers and government to counter cyber-threats and enhance the security of the Nation's cyberinfrastructure and capabilities. The outputs from its cybersecurity portfolio are 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.

NIST is extremely proud of its role in establishing and improving the comprehensive set of cybersecurity technical solutions, standards, guidelines, and best practices, and of the robust collaborations enjoyed with its federal government partners, private sector collaborators, and international colleagues.

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, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program cultivates trust in information technology and metrology 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.