Testimony of

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

United States House of Representatives

Committee on Science, Space and Technology

Subcommittee on Research and Technology

"The Expanding Cyber Threat"

January 27, 2015

Introduction

Chairwoman Comstock, Ranking Member 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 our role 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 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. Our 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). 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.

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

We employ collaborative partnerships with our customers and stakeholders to take advantage of their technical and operational insights and to leverage the resources of a global community. These collaborative efforts and our private sector collaborations in particular, are constantly being expanded by new initiatives, including in recent years through the National Strategy for Trusted Identities in Cyberspace (NSTIC), the National Cybersecurity Center of Excellence (NCCoE), in implementation of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," and the National Initiative for Cybersecurity Education (NICE).

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

NIST Cybersecurity Research, Standards and Guidelines

The NIST Special Publications and Interagency Reports provide management, operational, and technical security guidelines for Federal agency information systems, and cover a broad range of topics such as Basic Input/Output System (BIOS) management and measurement, key management and derivation, media sanitization, electronic authentication, security automation, Bluetooth and wireless protocols, incident handling and intrusion detection, malware, cloud computing, public key infrastructure, risk assessments, 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.

In addition, NIST maintains the National Vulnerability Database (NVD), a repository of standards-based vulnerability management reference data. The NVD makes available information on vulnerabilities, impact measurements, detection techniques, and remediation assistance. It provides reference data that enable government, industry and international security automation capabilities. The NVD also plays a role in the efforts of the Payment Card Industry (PCI) to identify and mitigate vulnerabilities. The PCI uses the NVD vulnerability metrics to discern the IT vulnerability in point-of-sale devices and determine what risks are unacceptable for that industry.

NIST researchers develop and standardize cryptographic mechanisms that are used throughout the world to protect information at rest and in transit. These mechanisms provide security services, such as confidentiality, integrity, authentication, non-repudiation and digital signatures, to protect sensitive information. The NIST algorithms and associated cryptographic guidelines are developed in a transparent and inclusive process, leveraging cryptographic expertise around the world. The results are in standard, interoperable cryptographic mechanisms that can be used by all industries.

NIST has a complementary program, in coordination with the Government of Canada, to certify independent commercial calibration laboratories to test commercially available IT cryptographic modules, to ensure that they have implemented the NIST cryptographic standards and guidelines correctly. These testing laboratories exist around the globe and test hundreds of individual cryptographic modules yearly.

Recently, NIST initiated a research program in usability of cybersecurity, focused on passwords and password policies; user perceptions of cybersecurity risk and privacy concerns; and privacy in general. The concept of “usability” refers generally to “the effectiveness, efficiency, and satisfaction with which the intended users can achieve

their tasks in the intended context of product use."[2] NIST's hope is that this usability research will lead to standards and guidelines for improving cybersecurity through increased attention to user interactions with security technologies.

NIST Engagement with Industry

It is important to note that the impact of NIST's activities under FISMA extend beyond providing the means to protect Federal IT systems. They provide the cybersecurity foundations for the public trust that is essential to our realization of the national and global productivity and innovation potential of electronic business and its attendant economic benefits. Many organizations voluntarily follow NIST standards and guidelines, reflecting their wide acceptance throughout the world.

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. 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 works extensively in smart card standards, guidelines and best practices. NIST developed the standard for the US Government Personal Identity Verification (PIV) Card, and actively works with the ANSI and the ISO on global cybersecurity standards for use in smart cards, smart card cryptography and the standards for the international integrated circuit card. [ANSI 504; ISO 7816 and ISO 24727]

NIST also conducts cybersecurity research and development in forward looking technology areas, such as security for federal mobile environments and techniques for measuring and managing security. These efforts focus on improving the trustworthiness of IT components such as claimed identities, data, hardware, and software for networks and devices. Additional research areas include developing approaches to balancing safety, security, and reliability in the nation's information and

[2] International Organization for Standardization (ISO), ISO 9241-11 (1998): "Ergonomic requirements for office work with visual display terminals (VDTs) – Guidance on usability."

communications technology supply chain; enabling mobile device and application security; securing the nation's cyber-physical systems and public safety networks; enabling continuous security monitoring; providing advanced security measurements and testing; investigating security analytics and big data; developing standards, modeling, and measurements to achieve end-to-end security over heterogeneous, multi-domain networks; and investigating technologies for detection of anomalous behavior and quarantines.

In addition, 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 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.

The 2013 Data Breach Investigations Report 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 the compromised credential of one of its business partners was the vector 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 13 pilots to help jumpstart the marketplace and test new approaches to overcome barriers, such as usability, privacy and interoperability, which have hindered market acceptance and wider use of stronger authentication technologies.

NSTIC exemplifies NIST's robust collaboration with industry, in large part, because the initiative calls on the private sector to play a lead role in its implementation. NIST has partnered with a privately led Identity Ecosystem Steering Group (IDESG) to craft better standards and tools 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. Recently, NIST established the Nation's first Federally Funded Research and Development Center (FFRDC) dedicated to cybersecurity to support the NCCoE. The center is a vehicle for NIST to work directly with businesses across

various industry sectors on applied solutions to 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.

Today NIST's NCCoE is working with government and industry partners on a number of projects including the Security Exchange of Electronic Health Information. This project focuses on securely exchanging information through the use of mobile devices. NIST plans to publish a practice guide for this project in the near future which will provide members of the technology community the materials list, configuration settings and other information they need to replicate this standards-based security solution.

Cybersecurity Framework

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." 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.

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. The Framework continues to be voluntarily implemented by industry and adopted by infrastructure sectors, and this is contributing to reducing cyber risks to our Nation's critical infrastructure.

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 cybersecurity, including in our Nation's critical infrastructure.

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

We at NIST recognize that we have an essential role to play in helping industry, consumers and government to counter cyber threats. 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 Federal government agencies and companies involved with critical infrastructure.

We are extremely proud of our role in establishing and improving the comprehensive set of cybersecurity technical solutions, standards, guidelines, and best practices and the robust collaborations with our 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, 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.