Testimony of

Kevin Stine

Leader, Security Outreach and Integration Group

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

United States Department of Commerce

Before the

United States Senate

Committee on Commerce, Science and Transportation

‘‘Confronting the Challenge of Cybersecurity’’

September 3, 2015

Introduction

Chairman Thune, members of the Committee, I am Kevin Stine, Leader of the Security Outreach and Integration Group in the Computer Security Division, 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 role in confronting the challenge of 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, 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 et seq.) 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. On behalf of NIST, I want to thank the Chairman for his steadfast leadership on this issue. The bill could not have been enacted into law without his efforts.

NIST accomplishes its mission in cybersecurity through collaborative partnerships with our customers and stakeholders in industry, government, academia, standards bodies, consortia and international partners. NIST employs these collaborative partnerships to take advantage of the technical and operational insights of our partners 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), the National Initiative for Cybersecurity Education (NICE), and through the implementation of the Obama Administration's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." These programs and others are supported by and implemented through NIST's cybersecurity research, standards, and guidelines.

NIST Cybersecurity Research, Standards, and Guidelines

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, online identity, authentication, access control, privacy risk management, 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 future 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 assists/helps/enables 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.

Pursuant to the Cybersecurity Research and Development Act of 2002, NIST also maintains a library of security setting configurations, also known as "checklists," for IT products used throughout the Federal government. This initiative is known as the National Checklist Program. Through the program, product vendors, as well as Federal contributors, supply checklists to be quality assured by NIST and peer-reviewed by the public, with the final benchmarks cataloged by NIST and made available as reference data for both government and the private sector. One of the more prominent examples of a checklist is the United States Government Configuration Baseline, or USGCB. To produce a USGCB, Federal checklist contributors work with the Federal CIO Council and NIST to determine government-wide security settings. The resulting USGCB checklists are made available to all parties through the National Checklist Program.

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. For example, with approval of the Secretary of Commerce, NIST recently published Federal Information Processing Standard (FIPS) 202, which specifies the SHA-3 family of hash functions that provide many important information security applications, including the generation and derivation of digital signatures.

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."[1] This usability research will lead to standards and guidelines for improving cybersecurity through

[1] ISO 9241-210:2010, *Ergonomics of human-system interaction – Part 210: Human-centered design for interactive systems*.

increased attention to user interactions with security technologies.

NIST Engagement with Government

In support of FISMA implementation, NIST continues its collaboration with the Department of Defense, the intelligence community, and the Committee on National Security Systems, through a Joint Task Force Initiative, to develop key cybersecurity guidelines for protecting U.S. Government information and information systems.

This collaboration allows the most broad-based and comprehensive set of safeguards and countermeasures ever developed for information systems. This unified framework of guidelines and recommendations 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.

Our set of standards, guidelines, and recommendations provide a standardized and repeatable framework for managing risk, called the Risk Management Framework. The Risk Management Framework provides a structured, yet flexible, approach for managing the risk resulting from using information systems to achieve the mission and business processes of an organization. The risk management concepts are intentionally broad-based with the specific details of assessing risk and employing appropriate risk mitigation strategies provided by supporting NIST information security standards and guidelines.

This approach allows for implementation of cost-effective, risk-based information security programs. It establishes a level of security due diligence for Federal agencies and contractors supporting the Federal government. It creates a consistent and cost-effective application of security controls across an information technology infrastructure and a consistent, comparable, and repeatable security control assessment. When implemented, it gives an organization a better understanding of enterprise-wide mission risks resulting from the operation of information systems.

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 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 Departments of Defense, State, and Homeland Security to coordinate positions on standards issues and priorities with the private sector through consensus standards organizations such as the American National Standards Institute (ANSI), the Joint Technical Committee 1 (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics

Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunications Union's Standardization Sector (ITU-T).

NIST's 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 U.S. Government Personal Identity Verification (PIV) Card (FIPS 201), and actively works with the ANSI and JTC 1 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 information 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 communications technology supply chain; enabling mobile device and application security; securing the nation's cyber-physical systems and public safety networks; enabling continuous information security monitoring; providing advanced information security measurements and testing; investigating information security analytics and big data; developing standards, modeling, and measurements to achieve end-to-end information 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 build trust among those creating and those using the solutions throughout the country.

International Cybersecurity Standardization

The Cybersecurity Enhancement Act of 2014 directed NIST to work with relevant Federal agencies to ensure interagency coordination in "the development of international technical standards related to information system security" and "ensure consultation with appropriate private sector stakeholders." It also called for NIST to submit a plan for ensuring the Federal agency coordination to Congress within one year. The International Cybersecurity Standards Working Group, which is led by the Department of Commerce/NIST, was set up by the National Security Council's Cyber Interagency Policy Committee to draft this plan, which will also serve as the basis of the required report to Congress.

The U.S. standards system differs significantly from the government-directed and government-led systems common in many other countries. Under the U.S. system, hundreds of standards development organizations (SDOs) provide the infrastructure for the preparation of standards documents. While these organizations are overwhelmingly private sector, government personnel

participate in standards development activities as equal partners along with representatives from industry, academia, and other organizations and consumers.

The new draft *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (NIST draft Interagency Report 8074)[2] and supplement lay out strategic objectives and recommendations for enhancing the U.S. government's coordination and participation in the development and use of international standards for cybersecurity. The draft report recommends the government make greater effort to coordinate the participation of its employees in international cybersecurity standards development to promote the cybersecurity and resilience of U.S. information and communications systems and supporting infrastructures.

A supplement[3] to the draft report provides a summary of ongoing activities in critical international cybersecurity standardization and an inventory of U.S. government and private sector engagement. It also provides guidance for agencies to plan and coordinate more effective participation in these activities.

The draft report supports the 2010 United States Standards Strategy,[4] which was developed through a public-private partnership and outlines the contribution of private-sector led standards development to overall competition and innovation in the U.S. economy and the imperative of public and private sector participation and collaboration.

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 works to address one of the most commonly exploited vectors of attack in cyberspace: the inadequacy of passwords for authentication.

Weak authentication and identity proofing methods continue to represent a disproportionate share of data breaches and other successful attacks. The 2013 Data Breach Investigations Report[5] noted that in 2012, 76% of network intrusions exploited weak or stolen credentials. In line with the results of this report, many recent high profile compromises involved weak or compromised credentials or weaknesses in identity proofing as the vector of attack.

NSTIC works 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 15 pilot programs to 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 lead implementation. NIST has partnered with the privately led Identity Ecosystem Steering Group (IDESG) to craft better standards and tools to improve authentication

---

[2] http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol1_draft_report.pdf

[3] http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol2_draft_supplemental-information.pdf

[4] http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/NSSC/USSS_Third_edition/USSS%202010-sm.pdf

[5] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

online.

National Cybersecurity Center of Excellence

In 2012, NIST established the National Cybersecurity Center of Excellence (NCCoE). The NCCoE brings together experts from industry, government, and academia to develop and transfer practical cybersecurity standards, technologies, and best practices to the nation's business sectors. By accelerating dissemination and use of standards, best practices, and integrated tools and technologies for protecting information technology assets and processes, the NCCoE fosters trust in U.S. business sectors and improvements to the overall security of the economy. The NCCoE supports implementation of existing cybersecurity guidelines and frameworks, serves as a technical resource for both public and private sectors, and contributes to the development of cybersecurity practices and practitioners.

The NCCoE is a unique partnership among three levels of government: NIST at the Federal level, the State of Maryland, and Montgomery County, Maryland. In addition the NCCoE established a Federally Funded Research and Development Center (FFRDC), the country's first FFRDC dedicated to cybersecurity, which helps the center respond to national priorities and critical security concerns impacting critical infrastructure, e-commerce, and privacy.

To date, NIST has established partnerships with 22 industry partners who have pledged to have a continuous presence at the center as National Cybersecurity Excellence Partner (NCEP) companies. In addition to these core partners, there are more than 25 other technology companies that are working on projects at the NCCoE under Cooperative Research and Development Agreements (CRADAs). These partners and collaborators support the NCCoE with hardware, software, and expertise. They provide the Center equipment to outfit labs as real-world environments, and their personnel work at the NCCoE as guest researchers.

Today, the NCCoE has programs working with the health care, energy, financial services, and retail sectors. In addition, the Center is addressing challenges that cut across sectors, including mobile device security, software asset management, cloud security, identity management, and secure email. The NCCoE's first practice guide,[6] released this summer for public comment, helps secure electronic health records on mobile devices. As both electronic medical records and mobile devices are increasingly used by health care practitioners, patient information needs to be protected to preserve privacy and safeguard identity and patient care. The NCCoE's practice guide, *Securing Electronic Health Records on Mobile Devices*, provides a detailed architecture and instructions so that IT professionals can recreate the security capabilities of the example solution. The guide does not recommend specific products, but provides a blueprint for the deployment and use of standards based technologies that address critical security concerns. The solution aligns to standards and best practices from NIST and to the Health Insurance Portability and Accountability Act Security Rule.

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.

Established in 2010, the National Initiative for Cybersecurity Education (NICE) promotes an ecosystem of cybersecurity education, training, and workforce development that effectively secures

[6] https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices

cyberspace. Led by NIST, NICE is a partnership between government, academia, and industry that builds upon existing successful programs, including the DHS/NSA Centers of Academic Excellence for Cybersecurity, and facilitates innovation to increase the supply of qualified cybersecurity workers.

NICE's emerging strategic priorities include accelerating learning and skills development, nurturing a diverse learning community, and guiding career development and workforce planning. NICE works to instill a sense of urgency in both the public and private sectors to address the skilled workforce shortage. It is also working to strengthen formal education programs, promote different academic pathways, and increase the participation of women, minorities, and veterans in the cybersecurity profession. Finally, it supports job seekers and employers to address market demands and maximize talent management.

NICE is also aligned with the President's Job-Driven Training Initiative and the Secretary of Commerce's Skills for Business Initiative that is partnering with business to equip workers for 21st century careers.

Cybersecurity Framework

Over one year ago, NIST issued the Framework for Improving Critical Infrastructure Cybersecurity (Framework)[7] in accordance with Section 7 of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."[8] The Framework, created through collaboration with industry, government, and academia, 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, which is contributing to reducing cyber risks to our Nation's critical infrastructure.

NIST supports Framework awareness and understanding by addressing a variety of sectors and communities through speaking engagements and meetings. NIST continues to educate other nations about the value of the Framework and the processes by which it was developed. Many of those nations are adopting Framework principles into equivalent national frameworks, while some are adopting the Framework in its entirety. To better support industry understanding and use, NIST is now publishing frequently asked questions and industry resources at the Framework Web site[9].

Pursuant to the Cybersecurity Enhancement Act of 2014, NIST also convened meetings with regulators to discuss application of the Framework within the cyber ecosystem, and the need for the Framework to remain a voluntary methodology, adaptable to the critical infrastructure risk and mission objectives. NIST participated in an advisory role to the Federal Communications Commission (FCC) Communications, Security, Reliability and Interoperability Council's (CSRIC)

---

[7] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[8] https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[9] http://www.nist.gov/cyberframework/index.cfm

Working Group 4. NIST is also an advisory member of the Cybersecurity Forum for Independent and Executive Branch Regulators. The forum was chartered to increase the overall effectiveness and consistency of regulatory authorities' cybersecurity efforts pertaining to U.S. Critical Infrastructure. In all of these interactions, NIST continues to communicate the merits of the voluntary Framework as an organizational and communication tool to better manage cybersecurity risk.

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 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.

Kevin Stine

Mr. Kevin Stine is the Leader of the Security Outreach and Integration Group in the Information Technology Laboratory's Computer Security Division at the National Institute of Standards and Technology. In this capacity, he oversees NIST collaborations with industry, academia, and government on the mission-specific application of security standards, guidelines, and technologies to help organizations understand and manage cybersecurity risk. This group develops technical cybersecurity guidelines and tools in diverse areas such as public safety communications; health information technology; smart grid, cyber physical, and industrial control systems; supply chain risk management; and federal agency cybersecurity programs. The group is also home to the National Initiative for Cybersecurity Education (NICE) and programs focused on cybersecurity outreach to small businesses, security education and training professionals, and federal agencies. Recently, he led NIST's efforts to develop the Framework for Reducing Cybersecurity Risk to Critical Infrastructure (Cybersecurity Framework) as directed in Executive Order 13636. He is past chair of the Federal Computer Security Managers' Forum, which promotes sharing of information security practices among federal agencies. He holds undergraduate degrees in Information Systems Management and Psychology from the University of Maryland, Baltimore County.