

Testimony of

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

Jointly before the
United States House of Representatives
Committee on Science

Subcommittee on Oversight
and
Subcommittee on Research and Technology

*“Can Technology Protect Americans from International
Cybercriminals?”*

March 4, 2014

Introduction

Chairmen Broun and Bucshon, Ranking Members Maffei and Lipinski and Members of the Subcommittees, 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 and our perspective on the recent cybercriminal activities.

Background

Cybertheft can occur at a scale unlike physical crimes. It can have multiple victims and a much larger impact than would be possible in conventional criminal activity. As we know, one breach can affect thousands – if not millions - of citizens. Cybertheft also can be perpetrated at the speed of electronic transactions. This makes interception difficult and places a strong reliance on preventive security controls. They also can occur without the physical presence of the criminal. This is possible because we work and live in an increasingly interconnected digital world. This introduces jurisdiction, legal and policy complexities as well as difficulty in attribution to the criminals themselves.

In response to the title of the hearing: "Can Technology Protect Americans from International Cybercriminals?" – my response would be: technology alone cannot solve these problems. However, we do believe that effective use of technology can make it more difficult for criminals to perpetrate these crimes, can make it easier for organizations to recover from serious incidents, and can, in some cases, prevent such incidents from occurring.

For example, technology can make it difficult to clone payment cards with stolen credentials or use the information to make online purchases. Smart cards using chip-and-pin technologies can make theft of the information stored on the card more difficult; however, often the attacks and exploits are not on the cards themselves, but are instead against the supporting payment infrastructure. We believe it takes a holistic approach that includes technology, training and awareness, policy, legal, economic and international efforts, to bring cybertheft, one of many different cyberthreats we face, under control.

With that background, today I would like to discuss some of NIST's activities that accelerate the development and deployment of security technologies and assist the US Government and other stakeholders and partners in protecting their information and communications infrastructure against cyberthreats, including cybertheft.

The Role of NIST in Cybersecurity

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. Our work in addressing technical challenges related to national priorities has ranged from projects related to the Smart Grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips.

In the area of cybersecurity, we have 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 information systems against threats to the confidentiality, integrity and availability of information and services, was strengthened through the Computer Security Act of 1987 and reaffirmed through the Federal Information Security Management Act of 2002 (FISMA).

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

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 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 Initiative for Cybersecurity Education (NICE), the National Strategy for Trusted Identities in Cyberspace (NSTIC), the National Cybersecurity Center of Excellence (NCCoE), and in implementation of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."

NIST Cybersecurity Research, Standards and Guidelines

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

The NIST Special Publications and Interagency Reports provide those management, operational, and technical security guidelines for Federal agencies 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.

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 Electronic 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, reliability in the nation's supply chain; enabling mobile device and application security; securing the nation's cyber-physical systems; 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.

Cybersecurity Framework

As you know, NIST has spent the last year working to convene the US Critical Infrastructure sectors to build a Cybersecurity Framework as part of Executive Order 13636. The Cybersecurity Framework, released last month, was created through

collaboration between industry and government, and 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. The Framework is already being implemented by industry, adopted by infrastructure sectors and is reducing cyber risks to our critical infrastructure, including the finance industry.

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 (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 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 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 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.

NIST and the NCCOE work extensively in standards and guidelines, as well as research and development in hardware roots of trust. Stronger security assurances can be possible by grounding security mechanisms in roots of trust. Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware

so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust.

In 2013, NIST and the NCCOE worked with government and industry partners on guidelines for hardware-rooted security features in mobile devices. These guidelines focus on device integrity, isolation, and protected storage features that are supported by roots of trust, and we continue our work to protect fundamental system firmware, commonly known as the BIOS. NIST continues working with key members of the computer industry on the use of roots of trust to improve the security of BIOS, computers and systems overall.

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 entities to counter cybertheft and cyberthreats. We look forward to continuing our work, along with our federal government partners, our private sector collaborators, and our international colleagues to establish and continually improve the comprehensive set of technical solutions, standards, guidelines, and best practices necessary to realize this vision.

Thank you for the opportunity to testify today on NIST's work in cybersecurity, and to share some of the specific work we do to assist organizations in reducing risks due to cybertheft. 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 is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of \$120 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.