Testimony of

Donna Dodson
Chief Cybersecurity Advisor
Director, National Cybersecurity Center of Excellence
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 Oversight

"*Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government*"

October 25, 2017

Introduction

Chairman LaHood, Ranking Member Beyer, and members of the Subcommittee, I am Donna Dodson, Director of the National Cybersecurity Center of Excellence and Chief Cybersecurity Advisor 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, I will discuss NIST's activities in support of the cybersecurity Framework and NIST's cybersecurity portfolio.

NIST's Role in Cybersecurity

NIST is a non-regulatory agency with the mission to promote U.S. innovation and industrial competitiveness in ways that enhance economic security and improve our quality of life. As a non-regulatory agency, NIST leverages its deep technical expertise, as well as its power as a convener of stakeholders from government, academia, and the private sector to develop and improve solutions to a wide range of technical and policy cybersecurity challenges.

One of NIST's key roles is to research, develop, and deploy information security standards and technology to protect the Federal Government's information systems against threats to confidentiality, integrity, and availability. Such efforts were strengthened through the Computer Security Act of 1987 (*Public Law 100-235*), broadened through the Federal Information Security Management Act of 2002 (FISMA*) (Public Law 107-347*), and reaffirmed in the Federal Information Security Modernization Act of 2014 (*Public Law 113-283*). The Cybersecurity Enhancement Act of 2014 (*Public Law 113-274*) further authorized NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

To address cybersecurity issues, NIST has long worked effectively with industry and federal agencies to help protect the confidentiality, integrity, and availability of information systems. NIST's Information Technology Laboratory (ITL) develops and deploys standards, tests, and metrics to make the nation's information systems more secure, usable, interoperable, and reliable. Our work in the cybersecurity area covers program areas including configuration and vulnerability management, cryptography, cybersecurity education and workforce development, identity and access management and risk management.

In addition to providing resources that organizations of all sizes can use to manage cybersecurity risk, NIST also provides resources to help organizations recover quickly from cybersecurity attacks with confidence that the recovered data is accurate, complete, and free of malware and that the recovered system trustworthy and fully capable to again function as originally designed. Some of NIST's critical cybersecurity resources are described below.

NIST's Cybersecurity Framework

In 2014, NIST issued the *Framework for Improving Critical Infrastructure Cybersecurity*[1] (Framework), which NIST created in collaboration with industry, academia, and other

[1] https://www.nist.gov/cyberframework

government agencies. The Framework consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure, such as the information technology, transportation, energy, healthcare, and financial services sectors. The voluntary, risk-based, flexible, repeatable, and cost-effective approach of the Framework helps those who use the Framework to manage cybersecurity risk. The Framework was originally designed to help protect critical infrastructure, but numerous business of all sizes and from many economic sectors now use the Framework to manage their cybersecurity risks, such as for supply chain risk management as described below.

Since publishing the Framework, NIST has released the NIST Interagency Report (NISTIR) *Small Business Information Security: The Fundamentals* (NISTIR 7621) to help small businesses understand and manage their cybersecurity risks.

Under Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, signed by President Trump on May 11, 2017, every Federal agency or department has to manage their cybersecurity risk by using the Framework and provide a risk management report to the Director of the Office of Management and Budget and to the Secretary of Homeland Security.

NIST also released a draft NISTIR, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies* (NISTIR 8170). This report helps federal agencies use the Framework, in conjunction with an extensive set of NIST cybersecurity risk management standards, guidelines, and controls, to manage their cybersecurity risks. Currently, NIST is in the process of updating the Framework, a process NIST plans to finalize in 2018.

NIST collaborates with the Department of Homeland Security's (DHS) Critical Infrastructure Cyber Community Voluntary Program to promote Framework implementation within the critical infrastructure sectors. NIST and DHS coordinate on a range of events promoting Framework implementation and understanding, such as webinars and workshops.

Supply Chain Risk Management

The Cybersecurity Framework also provides guidance for the security of the supply chain and to reduce supply chain threats to businesses and the manufacturing sector. The number of information and communication technologies is rapidly increasing and becoming more capable and complex every day. These technologies rely on a supply-chain ecosystem that is long, complex, variable, interconnected, globally distributed, and geographically diverse. Many organizations outsource the development, maintenance, and management of this ecosystem.

Because of this outsourcing, organizations—including federal agencies—are increasingly at risk of supply chain compromise. The same factors that decrease cost, enable interoperability, foster rapid innovation, and provide other benefits, also increase cyber supply chain risks. Managing supply chain risk requires an organization to ensure the integrity, security, and resilience of its supply chain.

NIST developed the Supply Chain Risk Management Program to work with industry, academia, and government to identify and evaluate effective technologies, tools, techniques, practices, and standards that help secure an organization's supply chain. This program examines the supply-chain risk throughout the entire lifecycle of systems, products, and services.

NIST is currently working to describe a structured method of prioritizing systems and components based on their relationship to an organization's mission, thereby enabling organizations to most efficiently deploy their resources.

Cryptography

NIST began its work on cryptography in 1972 and its importance is reflected in the growth of this work today. Under FISMA, NIST is responsible for developing standards and guidelines to protect non-national security federal information systems and the information they process. Our Cryptographic Technology Group (CTG) researches, analyzes, and standardizes cryptographic techniques and technologies, while encouraging innovation and helping technology users manage risks.

Although Federal Information Processing Standards (FIPS) apply to federal information systems, many private sector organizations voluntarily rely on them to protect sensitive personal and business information.

The Cryptographic Technology Group is developing its standards using an open and transparent process. The CTG conducts workshops and requests input and comments from government agencies, private industry, academia, and the global cryptographic community. We make such comments available publicly in the interest of transparency, trust, and to promote future research. The CTG examines each of its standards on a regular basis to determine if they need to be revised, withdrawn, or re-opened for public comment and, when appropriate, possible revision.

In addition to developing these standards, NIST runs the Cryptographic Module Validation Program, which validates the test results of a vendor's cryptographic modules to NIST FIPS 140-2. Laboratories accredited under the program test any company's cryptography to determine whether it meets NIST's cryptographic standards. NIST does not "pick winners and losers" among potential vendors. Rather, private-sector accredited testing laboratories conduct testing under this program that simply confirms whether a company's underlying cryptography works and technically meets the standard—nothing more and nothing less. As with the FIPS standards themselves, many private sector organizations worldwide rely upon this testing program for assurance that the cryptographic products they purchase meet NIST standards. To date, under this voluntary testing program, over 3000 cryptographic modules have been successfully validated under this program.

The National Vulnerability Database

Protecting information technology is critical and NIST plays a key role in this area by maintaining the repository of all known and publicly reported information technology

vulnerabilities, called the National Vulnerability Database (NVD). The NVD is an authoritative source for standardized information on security vulnerabilities that NIST updates regularly.

These vulnerabilities catalogued in the NVD are weaknesses in coding found in software and hardware that, if exploited, can impact the confidentiality, integrity, or availability of information or information systems. The NVD tracks vulnerabilities over time and allows users to assess changes in vulnerability discovery rates within specific products or specific types of vulnerabilities.

As part of maintaining the NVD, NIST works with organizations that apply to become a Common Vulnerabilities and Exposures (CVE) Numbering Authority, which allows an organization to publicly disclose a vulnerability with a preassigned CVE ID number, rather than be required to request a new number every time it discovers a new vulnerability. NIST also analyzes and provides a severity metric to assist practitioners in responding to each vulnerability.

National Software Reference Library

NIST, along with the Department of Homeland Security, and other federal, state, and local law enforcement agencies, supports the National Software Reference Library (NSRL). The NSRL collects digital signatures of software so that an organization can efficiently search its networks for that software and determine if and where the software is deployed. In a sense, the NSRL is like a fingerprint database for computer files; however, rather than helping a detective identify a person, it helps an organization quickly find a piece of software. In effect, the NSRL promotes efficient and effective use of computer technology in the investigation of crimes involving computers.

The NSRL collects software from various sources and incorporates profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and private industry to review files on a computer by matching profiles in the RDS. This process helps alleviate much of the effort involved in determining which files on a computer are important evidence or which files are already part of a criminal investigation. This ability reduces the number of files which must be manually examined, reducing the time and other resources law enforcement officials need to commit to a single incident.

Other stakeholders, such as businesses and other government agencies, use the NSRL RDS as part of their routine IT operations to ensure there are no malicious or unverified files on their systems.

Conclusion

The programs that I have mentioned here are only a portion of NIST's portfolio in cybersecurity, which is only a portion of what NIST does more broadly. NIST's work to provide and improve technical and policy solutions to an ever-growing set of cybersecurity challenges continues to grow. Thank you for the opportunity to testify today on NIST's work in cybersecurity. I am happy to answer any questions you may have.