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 Small Business

"*Small Business Cybersecurity: Federal Resources and Coordination*"

March 8, 2017

Introduction

Chairman Chabot, Ranking Member Velázquez, members of the Committee, 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). ITL cultivates trust in information technology and metrology through measurements, standards and testing. Thank you for the opportunity to appear before you today to discuss NIST's cybersecurity efforts as they relate to small businesses. Small businesses are more innovative, agile, and productive than ever, thanks to the capabilities delivered by information technology (IT), but the IT security challenge for small businesses looms larger than ever.

NIST Role 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.

NIST standards and guidelines are developed in an open, transparent, and collaborative manner that enlists broad expertise from around the world. While developed for federal agency use, these resources are often voluntarily adopted by other organizations, including small and medium-sized businesses, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective and accepted globally. NIST disseminates these resources through a variety of means that encourage the broad sharing of information security standards, guidelines, and practices, including outreach to stakeholders, participation in government and industry events, and online mechanisms.

Small Business Role

NIST recognizes that small businesses play an important role in the U.S. economy. These businesses produce approximately 46% of the Nation's private-sector output and create 63% of all new jobs in the country.[2] Since information technology is critical to the delivery of goods and services for all businesses, the importance of addressing risks associated with doing business in a cyber-environment cannot be overstated.

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347; 116 Stat. 2899).
[2] Small Business Administration, https://www.sba.gov/sites/default/files/FAQ_March_2014_0.pdf

Since nearly 99% of all U.S. businesses are small or medium-sized,[3] a vulnerability common to a large percentage of these organizations could pose a significant threat to the Nation's economy and overall security. Many of these businesses house sensitive personal information including healthcare or financial information. Many small businesses also provide services to the federal, state, local and tribal governments and have access to government information or systems. In the interconnected environment in which Americans currently operate, it is vital that small businesses are aware of and actively manage cyber risks.

When implementing new technologies, small businesses need to fully understand all of the potential security risks created by connecting to the Internet. The risks to systems are so complex and pervasive that one cannot reasonably expect small businesses to be experts in all areas of security, including properly implementing security controls for complex system configurations and assessing security features associated with new and emerging technology. Cybersecurity incidents can have a devastating effect on small businesses—60% of small companies will close within six months following a cyberattack.[4]

NIST has long worked effectively with industry and federal agencies to help protect the confidentiality, integrity, and availability of information systems. Ensuring that business-related information is secure is essential to the functioning of America's economy. NIST's broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users, including small- and medium sized businesses.

Cybersecurity Fundamentals

In November 2016, NIST released a major revision to the popular report *Small Business Information Security: The Fundamentals* (NIST Interagency Report, NISTIR 7621R1). The report is designed for small business owners with little cybersecurity expertise and provides basic steps needed to help protect their information systems. NISTIR 7621R1 guides readers through a simple risk assessment to understand the organization's vulnerabilities. After identifying and determining the value of the organization's information, the users evaluate the risk to the business and customers if its confidentiality, integrity, or availability were compromised.

The guide describes how to:

- Limit employee access to only appropriate data and information,
- Train employees about information security,
- Create policy and procedures for information security,
- Encrypt data,
- Install web and email filters, and
- Patch or update operating systems and applications.

NISTIR 7621R1 is also aligned with NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework), a set of voluntary standards, guidelines, and practices to promote the protection of our nation's critical infrastructure. NISTIR 7621R1 can be used as a step from cybersecurity fundamentals to more advanced cybersecurity risk management described in the Framework.

[3] Small Business Administration, https://www.sba.gov/sites/default/files/Whats_New_With_Small_Business.pdf.
[4] https://staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic

Cybersecurity Framework

NIST released the initial version of the Framework three years ago, 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 Framework's voluntary, risk-based, prioritized, flexible, repeatable, and cost-effective approach, developed for use by organizations – including small businesses – to help these organizations to manage cybersecurity-related risk. 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 the Nation's critical infrastructure. According to a June 2015 presentation by Khushbu Pratap and Earl Perkins of Gartner, Inc., by 2020, more than 50% of organizations will use the NIST Cybersecurity Framework, up from 30% in 2015.

Last month, NIST released a proposed 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 10th of this year, provides new details on managing supply chain risks, clarifies key terms, and introduces measurement methods for cybersecurity.

NIST collaborates with the Department of Homeland Security's Critical Infrastructure Cyber Communitty (C^3) Voluntary Program to promote Framework implementation among SMBs within the 16 sectors of critical infrastructure. NIST and DHS coordinate on a range of events promoting Framework implementation and understanding, such as webinars and workshops.

In addition to the Cybersecurity Framework, NIST has developed, over the past decade, an extensive set of security standards and guidelines, including a Risk Management Framework (RMF), that can be customized for small businesses and implemented on a voluntary basis to help protect a small business's intellectual property and organizational assets. The flexibility of the RMF is backed up by a set of comprehensive, state-of-the-practice security and privacy controls that can help small businesses be less susceptible to a range of cyber threats that can impact their competitiveness and survivability in a high risk, Internet-based operating environment.

Baldrige-Based Tool for Cybersecurity Excellence

Building further on the success of the Cybersecurity Framework, NIST released the draft Baldrige Cybersecurity Excellence Builder, a self-assessment tool to help organizations of all sizes better understand the effectiveness of their cybersecurity risk management efforts. The Builder blends the best of two globally recognized and widely used NIST resources: the organizational performance evaluation strategies from the Baldrige Performance Excellence Program and the risk management mechanisms of the Cybersecurity Framework. Using the Builder, organizations of all sizes and types can:

- Determine cybersecurity-related activities that are important to business strategy and the delivery of critical services;
- Prioritize investments in managing cybersecurity risk;

- Assess the effectiveness and efficiency in using cybersecurity standards, guidelines, and practices;
- Assess their cybersecurity results; and
- Identify priorities for improvement.

Like the Cybersecurity Framework, the Baldrige Cybersecurity Excellence Builder is adaptable to meet an organization's specific needs, goals, capabilities, and environments.

Interagency Collaborations

Since 2001, NIST has partnered with the Small Business Administration (SBA) and the Federal Bureau of Investigation's InfraGard program to sponsor computer security workshops and provide online support for small businesses. The workshops, which are held across the country, feature security experts who explain information security threats and vulnerabilities and describe protective tools and techniques which can be used to address potential security problems.

NIST, in cooperation with SBA and the Association for Small Business Development Centers, has participated in the annual conference of Small Business Development Centers, providing participants with information to increase awareness of NIST resources. In addition to its work with SBA and InfraGard, NIST is also working with the National Cyber Security Alliance (NCSA) to bring more online tools to small businesses on the NCSA's small business website[5].

In 2016, as part of the Cybersecurity National Action Plan (CNAP), NIST partnered with the Small Business Administration, the Federal Trade Commission, and the Department of Energy to develop and provide cybersecurity training webinars for small businesses. These webinars were attended by hundreds of small businesses and attendees from 68 SBA District Offices, nine NIST Hollings Manufacturing Extension Partnership program (MEP) Centers, and other regional networks across the country.

National Initiative for Cybersecurity Education

A cybersecurity educated workforce in all organizations is critical to improving the Nation's cybersecurity capabilities. Cybersecurity is particularly challenging for small businesses because they often have few, if any, staff devoted to IT or cybersecurity, and these staff tend to be generalists – not specialists. Alternatively, businesses outsource IT or cybersecurity functions and rely on third-party service providers. Consequently, the workforce needs of small businesses are both nuanced and unique.

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 United States. 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 for public comment to help our Nation more effectively identify, recruit, develop, and maintain its cybersecurity talent. The framework provides a common language to categorize and describe

[5] https://staysafeonline.org/business-safe-online/

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.

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 across the United States. The RAMPS work to bring together K-12 schools, community colleges, universities, training providers, economic development organizations, local and state government, and employers, especially from small and medium-sized businesses in the community, to coordinate regional activities addressing the cybersecurity workforce shortage and expand their local economy.

National Cybersecurity Center of Excellence

The National Cybersecurity Center of Excellence (NCCoE) turns standards and best practices into practical solutions to address some of the Nation's thorniest cybersecurity challenges. The NCCoE collaborates with experts from industry, academia, and government to create and promote solutions to real-world cybersecurity problems using commercially available products in the form of technical practice guides that can be used by organizations including small and medium-sized businesses. For example, the NCCoE project on Mobile Device Security provides guidance to small and medium-sized businesses on the implementation of capabilities to secure sensitive business data residing in the cloud and being accessed by employees on mobile devices.

Health care providers increasingly are using mobile devices to collect, access, process, and transmit patient information. The NCCoE project Securing Electronic Health Records on Mobile Devices provides guidance for healthcare organizations of all sizes seeking to improve the security of these ubiquitous devices. This guide can be used by local and regional hospitals as healthcare providers leverage mobile devices to the workplace. These projects and all of the work at the NCCoE help strengthen the security of the Nation's businesses.

Conclusion

Small businesses are more innovative, agile, and productive than ever, thanks to the capabilities delivered by information technology, but the IT security challenge for small businesses looms larger than ever. Systems managed by small businesses are part of a large, interconnected community enabled by extensive networks and increased computing power.

Small businesses must take steps to secure systems against malicious activity, or accidental unauthorized disclosure of sensitive information or breach of privacy.

NIST recognizes that it has an essential role to play in helping small businesses. The NIST programs described here demonstrate that NIST's cybersecurity portfolio is applicable to a wide variety of users, from small and medium-sized enterprises to large private and public organizations.

NIST is fiercely 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 present NIST's views regarding security challenges facing small enterprises. I will be pleased 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 that 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.