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 Senate

Committee on Small Business and Entrepreneurship

"Cyber Crime: An Existential Threat to Small Business"

March 13, 2019

Introduction

Chairman Rubio, Ranking Member Cardin, and members of the Committee, I am Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Today's hearing, "Cyber Crime: An Existential Threat to Small Business," addresses a topic of critical importance to America's small businesses, and consequently to the security and economic well-being of America as a whole. While Federal agencies other than NIST have the lead with respect to enforcement and other key aspects of cyber crime, I thank you for the opportunity to appear before you today to discuss NIST's role in helping small businesses to improve their cybersecurity.

NIST Role in Cybersecurity

Home to five Nobel Prizes, with programs focused on national priorities such as advanced manufacturing, the digital economy, precision metrology, quantum science, and biosciences, NIST's 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, when it helped develop and published the data encryption standard, which enabled efficiencies like electronic banking that we all enjoy today. 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) (Public Law 107-347)[1] and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 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 develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies as well as businesses of all sizes, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, state-of-art and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

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

NIST has a long-standing and on-going effort supporting small business cybersecurity, through its laboratory programs as well as its externally focused Hollings Manufacturing Extension Partnership (MEP) and Baldrige Performance Excellence (Baldrige) programs.

Small Business Role

NIST recognizes that small businesses play an important role in the U.S. economy. Small businesses comprise 99.9 percent of all firms, 97.6 percent of exporting firms, and 47.8 percent of private sector employees.[2] Small businesses accounted for 61.8 percent of net new jobs from the first quarter of 1993 until the third quarter of 2016.[3]

Cybersecurity is vitally important to a business' bottom line. Cybersecurity breaches cost businesses billions of dollars in lost revenue and loss of productivity every year. The impact on reputation and the loss of customers' trust can cause long-term damage to a small business. A vulnerability common to a large percentage of small businesses 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.

While many small businesses have limited resources, personnel, and understanding of cybersecurity risks, small businesses are not necessarily less secure. Because of their size, small businesses are frequently able to be more innovative and agile in their responses to cybersecurity risks than larger organizations. Small businesses can nimbly pivot, update and adapt to new policies, requirements, and 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.

NIST has a long-standing and on-going effort supporting small business cybersecurity. This is accomplished by providing guidance through publications, meetings, and events. ITL has worked with interagency partners, including the Small Business Administration (SBA), the Federal Trade Commission, Federal Bureau of Investigation's InfraGard program and DHS' Cybersecurity and Infrastructure Security Agency, or CISA, to host cybersecurity workshops, training webinars, and has provided online resources for small businesses. More recently, the NIST Small Business Cybersecurity Act,[4] which became law on August 14, 2018, directed NIST

[2] https://www.sba.gov/sites/default/files/advocacy/SB-FAQ-2017-WEB.pdf
[3] Id.
[4] Public Law No. 115-236; 15 U.S.C. § 272(e)(1)(A)(viii).

to "disseminate clear and concise resources to help small business concerns identify, assess, manage, and reduce their cybersecurity risks."

NIST Small Business Cybersecurity Corner

The vast majority of smaller businesses rely on information technology to run their businesses and to store, process, and transmit information. Protecting this information from unauthorized disclosure, modification, use, or deletion is essential for those companies and their customers. With limited resources and budgets, these companies need cybersecurity guidance, solutions, and training that is practical, actionable, and enables them to cost-effectively address and manage their cybersecurity risks.

The NIST Small Business Cybersecurity Corner[5] puts these key resources in one place. NIST actively collaborates with the Small Business Administration, CISA within the Department of Homeland Security, and Federal Trade Commission, each of which is a contributor to the NIST Small Business Cybersecurity Corner web site. These agencies, as well as non-profit organizations, are providing small business-focused resources to be shared through that site and they will promote awareness and use of the site.

All resources are free and draw from information produced by federal agencies, including NIST and several primary contributors, as well as non-profit organizations. The NIST Small Business Cybersecurity Corner will be expanded and updated regularly to include more government, non-profit organization, and some for-profit organization resources.

Cybersecurity Framework

I would like to highlight some changes to a document that the Committee may be familiar with: the Framework for Improving Critical Infrastructure Cybersecurity[6] (the "Cybersecurity Framework"), which many organizations—including many small businesses—use to manage their cybersecurity risk. Beginning in 2013, NIST created, promoted, and continues to enhance the Framework in collaboration with industry, academia, and other government agencies. The Framework provides a voluntary, risk-based, flexible, repeatable, and cost-effective approach that relies on voluntary standards, guidelines, and practices to help organizations identify, assess, manage, and communicate cybersecurity risks.

The Cybersecurity Framework was originally designed for owners and operators of critical infrastructure, but organizations of all sizes and from many economic sectors now use the Cybersecurity Framework to manage their cybersecurity risks, including risks to their supply chains. While use is both voluntary and widespread in the private sector, the May 2017 Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and

[5] https://www.nist.gov/itl/smallbusinesscyber
[6] https://www.nist.gov/cyberframework

Critical Infrastructure[7] formally requires agencies to use the Cybersecurity Framework to manage their cybersecurity risk—something many agencies did prior to its issuance.

In response to stakeholder requests, NIST began the public engagement process to update the Cybersecurity Framework. This process included NIST examining lessons learned from use of the Cybersecurity Framework, collecting written comments, hosting multiple workshops, incorporating comments and feedback, and issuing multiple drafts before publishing the final updated version 1.1 in April of 2018.[8] During the process, we engaged industry and stakeholders to ensure that the Cybersecurity Framework is scalable in many dimensions, and that enterprises ranging from large multinationals to small- and medium-sized businesses can use it to manage their cybersecurity risk, including to create a risk management program suitable for their needs. The Cybersecurity Framework continues to be a living document which draws strength from active and voluntary private-sector contributors.

Cybersecurity Fundamentals

In November 2016, NIST released a major revision to the popular report Small Business Information Security: The Fundamentals[9] (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.

NISTIR 7621R1 is organized according to the Cybersecurity Framework and can be used as a step from cybersecurity fundamentals to more advanced cybersecurity risk management described in the Cybersecurity Framework.

Risk Management Framework

In addition to the Cybersecurity Framework, NIST has developed, over the past decade, an extensive set of cybersecurity 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. NIST released the second version of Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations*,[10] in December 2018, after receiving

[7] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
[8] https://www.nist.gov/cyberframework/framework
[9] https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final
[10] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

over 500 comments from interested individuals and organizations. This update enhances the RMF in response to a May 2017 Executive Order, OMB Circular A-130, and two OMB memoranda.

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations.

NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*,[11] was developed in collaboration with the National Archives and Records Administration, the CUI executive agent, and the Department of Defense, which has small business partners across the country. It provides federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI:

- when such information is resident in nonfederal systems and organizations;
- when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and
- where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.

The security requirements apply to all components of nonfederal systems and organizations, including small businesses, that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Cybersecurity for Small U.S. Manufacturers

Small businesses constitute the backbone of the U.S. manufacturing sector, which is a major contributor to U.S. economic security. Within NIST, MEP has a specific focus on providing direct, hands-on technical assistance to small manufacturers. MEP operates a nationwide network of technical assistance, with MEP Centers located in every U.S. state and Puerto Rico.

MEP prioritizes providing awareness, training, and hands-on cybersecurity assistance to small manufacturers to help them implement protections to secure their business information and assets. Some small manufacturers may not perceive themselves as targets, yet they are frequently attacked as entry points into larger supply chains. MEP Centers around the Nation have engaged directly with small U.S. manufacturers in the commercial and defense markets through cybersecurity awareness events, workshops, webcasts and hands-on, direct technical assistance projects. MEP Centers have also focused on helping small, sub-tier defense contractors understand the cybersecurity requirements in the Defense Federal Acquisition Regulation Supplement (DFARS).

[11] https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

NIST MEP provides guidance and resources to MEP Centers across the country, to ensure technical accuracy when MEP Centers provide assistance related to the NIST Cybersecurity Framework and NIST Special Publications (SPs), and also to ensure that MEP Center assistance approaches are consistent with DoD policy intent when serving defense manufacturers. NIST MEP has published NIST Handbook 162, *NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements.*[12] This handbook is regularly used by MEP Centers to provide cybersecurity assistance to small manufacturers, and it has been downloaded nearly 42,000 times from the NIST website since its publication in November 2017.

Baldrige-Based Tool for Cybersecurity Excellence

Building further on the success of the Cybersecurity Framework, NIST released the draft Baldrige Cybersecurity Excellence Builder,[13] 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.

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

[12] https://www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security
[13] https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative#bceb

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 August 2017, NIST released NIST Special Publication 800-181, the *NICE Framework*,[14] which is a national resource that categorizes and describes cybersecurity work. The NICE Framework establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors and to help employers assess their cybersecurity workforce, identify critical gaps in cybersecurity staffing, and improve position descriptions. The NICE Challenge Project,[15] funded by NIST and developed and maintained by California State University, San Bernardino, is designed to create a flexible set of challenge environments and supporting infrastructure with a low barrier of use, in which one is able to perform the tasks outlined in the NICE Framework.

In 2016, CyberSeek,[16] an interactive online tool designed to help close the cybersecurity skills gap, was released to the public. Funded by NIST and developed by CompTIA in partnership with Burning Glass Technologies, CyberSeek provides a data visualization of the need for and supply of cybersecurity workers to guide employers, job seekers, policy makers, education and training providers, and guidance counselors. CyberSeek includes a cybersecurity Jobs Heat Map, which shows information on the supply of workers with relevant credentials. This project also shows career pathways in cybersecurity that map opportunities for advancement in the field.

National Cybersecurity Center of Excellence

Established in 2012, NIST's National Cybersecurity Center of Excellence (NCCoE)[17] is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges.

Through consortia under Cooperative Research and Development Agreements (CRADAs), including private sector collaborators—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. Working with communities of interest, the NCCoE has produced practical cybersecurity solutions that benefit large and small businesses, and third-party service providers in diverse sectors including healthcare, energy, financial services, retail, and manufacturing.

[14] https://csrc.nist.gov/publications/detail/sp/800-181/final
[15] https://www.nist.gov/itl/applied-cybersecurity/nice
[16] https://www.nist.gov/itl/applied-cybersecurity/nice/cyberseek
[17] https://www.nccoe.nist.gov/

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 cybersecurity challenges facing small businesses. 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 $160 million, nearly 400 employees, and approximately 300 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.