NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Testimony of

Kevin Stine
Chief, Applied Cybersecurity Division
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

"Cybersecurity: Challenges and Opportunities for Small Businesses"

Field Hearing

August 15, 2023

Introduction

Senator Hickenlooper and the Small Business and Entrepreneurship Committee, I am Kevin Stine, the Chief of the Applied Cybersecurity Division 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 NIST's role in helping small businesses to improve their cybersecurity.

Cybersecurity is one of many NIST programs that address critical national priorities. Others include artificial intelligence, advanced manufacturing, the digital economy, precision measurements, quantum science, biosciences, and a host of additional areas critical to our nation's success. The mission of NIST 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. NIST conducts research and provides services relied upon by companies of all sizes in all sectors of our economy. NIST also is home to five Nobel Prize winners in the most cutting-edge areas of science – three from our laboratories in Boulder, Colorado.

NIST's Role in Cybersecurity

In the area of cybersecurity, NIST has worked with federal agencies, industry, international partners, and academia since 1972, when it helped to develop and published the Data Encryption Standard, which enabled security with efficiencies, like the electronic banking that we all enjoy today. NIST's role is to provide standards, guidance, tools, data references, and testing methods to protect information systems against threats to the confidentiality, integrity, and availability of information and services. This role 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.

In developing its guidelines, NIST prides itself on the strong partnerships we have developed, and relies on an open, transparent, and collaborative process that enlists broad expertise from government, industry of all sizes, academia, and non-profit entities to develop and improve our cybersecurity resources. 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.

NIST's direct connections with companies and other users of our guidance advance our efforts to inform government and private sector cybersecurity-related policy decisions.

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

NIST's Role to Help Small Businesses Manage Cybersecurity Risk

NIST recognizes that small businesses play a vital role in the U.S. economy. Small businesses comprise 99.9% of all American businesses, generate 32.6% of known export value, and account for 46.4% of private sector employees[2]. Small businesses accounted for 62.7% of net jobs created from 1995-2021[3].

Cybersecurity can directly affect the bottom line of nearly every business. 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. Small businesses also provide services to the federal, state, local and tribal governments; have access to government information or systems; and make up a significant component of the nation's supply chain, providing goods and services to our public and private sectors. In the interconnected environment in which Americans currently operate, it is vital that small businesses are aware of and actively manage cyber risks – and that they can do that without undue burdens.

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 may be more innovative and agile in their responses to cybersecurity risks than larger organizations. They can pivot, update and adapt to new policies, requirements, and risks in a more timely manner than some larger organizations.

Like any other organization, especially when implementing new technologies, small businesses need to fully understand the potential security risks created by connecting to the Internet. The risks to systems are so complex and pervasive that it is not reasonable to 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. That is especially true with the explosion of Internet of Things (IoT) technologies.

NIST has a long-standing and continuing effort to help small businesses tackle their cybersecurity needs. For instance, NIST provides guidance through publications, meetings, and events. NIST has worked with interagency, industry, and non-profit partners to host cybersecurity workshops, training webinars, and provide online resources for small businesses.

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. Increasingly, these companies depend heavily on

[2] https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/

[3] https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/

IoT products and services. 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[4] puts these key resources in one place.

Congress has given NIST responsibility[5] through the NIST Small Business Cybersecurity Act (Public Law 115-236) to disseminate consistent, clear, concise, and actionable resources to small businesses to help them identify, assess, manage, and reduce their cybersecurity risks. NIST has created a variety of resources including short videos on topics such as multi-factor authentication and ransomware, and case studies that provide engaging, realistic scenarios that are based on actual small business cybersecurity incidents.

In addition to NIST-developed resources, the law directs NIST to consult other agencies, which NIST does and more. For starters, the Small Business Administration, Department of Homeland Security, and Federal Trade Commission are contributors to the NIST Small Business Cybersecurity Corner web site. They are providing small business-focused resources to be shared through that site, and we expect they will promote its awareness and use. All resources are free and draw from information produced by federal agencies, including NIST as well as non-profit organizations. The Small Business Cybersecurity Corner is expanded and updated regularly to include more government and non-profit organizations' resources.

Small Business Cybersecurity Community of Interest

In March 2023, NIST launched the Small Business Cybersecurity Community of Interest (COI) to convene companies, trade associations, and others who can share business insights, expertise, challenges, and perspectives to guide our work and assist NIST to better meet the cybersecurity needs of small businesses.

Sometimes small businesses lack guidance appropriate to their priority needs and capabilities. Other times there is simply too much information available, and they have difficulty knowing where to start or what is most important to best manage cybersecurity risks. And sometimes that information is too complex. A small business faced with any of these prospects can be overwhelmed and, consequently, may not act. The same often holds true for smaller non-profits, educational institutions, and government agencies.

The NIST Small Business Cybersecurity COI gives small companies and those speaking on their behalf the opportunity to inform NIST's National Cybersecurity Center of Excellence (NCCoE) and NIST more broadly about how we can best serve their needs by guiding the agency's efforts and tailoring the resources that we produce so that those can be effectively and efficiently used by smaller organizations.

[4] https://www.nist.gov/itl/smallbusinesscyber

[5] https://www.congress.gov/115/plaws/publ236/PLAW-115publ236.pdf

Members of the COI will learn about NIST's current and planned resources intended for smaller organizations and provide feedback about the expected usefulness of these resources based on the realities of their business situations, settings, needs, and capabilities.

NIST Cybersecurity Framework

The Framework for Improving Critical Infrastructure Cybersecurity (the "Cybersecurity Framework" or "CSF") is a foundational and essential tool for all organizations—including many small businesses—to better understand, communicate, and reduce their cybersecurity risk.

Beginning in 2013, following an Executive Order and congressional legislation[6], NIST created, promoted, and continues to enhance the Cybersecurity Framework in collaboration with industry, academia, and other government agencies. It provides a voluntary, risk-based, flexible, repeatable, and cost-effective approach that consists of voluntary standards, guidelines, and practices to help organizations understand, assess, prioritize, 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. The Framework is also increasingly leveraged in governmental policies (at the federal, state, and international level) as a recommended or even required resource for organizations.

The Cybersecurity Framework is a living document that is refined, improved, and evolves over time. Regular updates help the Framework keep pace with technology and threat trends, integrate lessons learned, and move best practices to common practice. NIST initially produced the Framework in 2014 and updated it in April 2018 with CSF 1.1. Based on stakeholder feedback, in order to reflect the ever-evolving cybersecurity landscape and to help organizations more easily and effectively manage cybersecurity risk, NIST is working towards a new, more significant update to the Framework, which will be CSF 2.0.

On August 8, 2023, NIST issued a complete draft of CSF 2.0 for public comment. The process to develop this draft included NIST examining lessons learned from use of the Cybersecurity Framework, collecting written comments, hosting multiple workshops, and incorporating comments and feedback on prior drafts over the past year. During the drafting process we engaged diverse stakeholders to ensure that the Cybersecurity Framework is scalable in many dimensions, and that enterprises ranging from large multinationals to small and medium-sized organizations can use it to manage their cybersecurity risk. Commenters included Manufacturers Edge of Colorado, a partner of the NIST Manufacturing Extension Partnership which works with other organizations to provide resources, training, and more to the Colorado manufacturing community. Others weighing in on the next version of the Framework included the Western Governors' Association. We are using the Small Business Community of Interest to ensure smaller companies know about the proposed revision of the Framework.

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

[6] https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

The protection of Controlled Unclassified Information (CUI) in nonfederal systems and organizations is critical to federal agencies, as our nonfederal partners, including small businesses, require access to CUI to support federal government missions. NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, provides federal agencies with recommended security requirements for protecting the confidentiality of CUI.

The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. The responsibility of federal agencies to protect CUI does not change when the information is shared with nonfederal organizations. Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by nonfederal organizations of any size using nonfederal systems.

NIST has produced and is updating companion publications that provide an assessment methodology and assessment procedures.

Partnering to Provide Cybersecurity Assistance 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, the Manufacturing Extension Partnership (MEP) has a specific focus on providing direct, hands-on technical assistance to small and medium-sized manufacturers. MEP operates a nationwide network of technical assistance via 51 Centers, with one in every state and Puerto Rico.

MEP prioritizes providing awareness, training, and hands-on cybersecurity assistance to small and medium-sized manufacturers (SMMs) to help them secure their business information and assets. These smaller manufacturers are particularly vulnerable to cybersecurity attacks because they generally do 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 U.S. SMMs in the commercial and defense markets through cybersecurity awareness 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.

MEP's cybersecurity working group provides a forum for the MEP nationwide network to share their best practices and challenges in order to create new opportunities for SMMs. MEP continues to incorporate NIST laboratories' subject matter experts into the cybersecurity working group to stay up to date on cybersecurity practices for manufacturing.

Cybersecurity Workforce for Small Businesses

A skilled and diverse cybersecurity 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.

NICE – a public-private collaboration among government, academia, and industry – is a program led by NIST to enhance the overall cybersecurity education, training, and workforce development capabilities of the United States. NICE seeks to energize and promote a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development. As the lead agency for this initiative, NICE works with federal agencies, as well as with industry and academia, to ensure a digital economy enabled by a knowledgeable and skilled cybersecurity workforce.

The NICE Workforce Framework for Cybersecurity[7] is a national resource that establishes a taxonomy and common lexicon categorizing and describing cybersecurity work. The NICE Framework is intended to be applied in the public, private, and academic sectors to help employers assess their cybersecurity workforce, identify critical gaps in cybersecurity staffing, and improve position descriptions.

NIST also funds CyberSeek[8], an interactive online tool designed to help close the cybersecurity skills gap. 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.

These tools are helpful to large and small businesses alike, as well as to other organizations.

In September 2016, NICE awarded funding for five pilot programs – including the Cyber Prep Program at Pikes Peak Community College – to support Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development. Following the successful pilot program, NIST is again offering funding to establish RAMPS partnerships. Effective partnerships will focus on bringing together employers who have cybersecurity skill shortages with educators to focus on developing a skilled workforce to meet industry needs within local or regional economies. NIST is also a Founding Partner of the US Cyber Games to help with the recruitment, training, and development of the team representing the United States in international cybersecurity competitions.

National Cybersecurity Center of Excellence

Established in 2012, NIST's National Cybersecurity Center of Excellence (NCCoE) is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address cybersecurity challenges facing U.S. businesses. The Center provides standards-based, practical cybersecurity solutions by tailoring NIST's standards and guidance to develop real-world, actionable guidance for specific sectors and technologies. These use case

[7] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf
[8] https://www.cyberseek.org/

focused resources can help organizations of any size to leverage leading practices to reduce cybersecurity risk.

The NCCoE works closely with technology partners – from Fortune 50 market leaders to small companies specializing in IT security. The Center has developed leading cybersecurity practices for small manufacturers and for home Internet of Things devices. It also has developed profiles of the NIST Cybersecurity Framework for specific use-cases, including to protect against ransomware as well as to secure space systems, election infrastructure, electric vehicle charging, and liquified natural gas.

Conclusion

Small businesses are more innovative, agile, and productive than ever, thanks to the capabilities delivered by information technology, but the cybersecurity 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 has an essential role to play in helping small businesses. NIST's cybersecurity portfolio applies to a wide variety of users, from small and medium-sized enterprises to large private and public organizations.

NIST is proud of its role in establishing and improving the comprehensive set of cybersecurity technical solutions, standards, guidelines, and best practices – and the policy decisions which are informed by that work. Our agency is especially proud of the robust collaborations enjoyed with Federal government partners, private sector collaborators of all sizes, academia, and international colleagues.

Thank you for the opportunity to present NIST's work on cybersecurity challenges facing small businesses. I will be pleased to answer any questions you may have.

Kevin Stine

Mr. Kevin Stine is the Chief of the Applied Cybersecurity Division in the National Institute of Standards and Technology's Information Technology Laboratory (ITL). He is also NIST's Chief Cybersecurity Advisor and Associate Director for Cybersecurity in NIST's ITL. In these roles, he leads NIST collaborations with industry, academia, and government to improve cybersecurity and privacy risk management through the development and effective application of standards, best practices, and technologies. The Applied Cybersecurity Division develops cybersecurity and privacy guidelines, tools, and reference architectures in diverse areas such as public safety communications; health information technology; smart grid, cyber physical, and industrial control systems; and programs focused on outreach to small businesses and federal agencies. The Division is home to several priority programs including the National Cybersecurity Center of Excellence, Cybersecurity Framework, Cybersecurity for IoT, Identity and Access Management, Privacy Engineering and Risk Management, and the National Initiative for Cybersecurity Education.