

**CYBERSECURITY: CHALLENGES AND  
OPPORTUNITIES FOR SMALL BUSINESSES**

---

---

**HEARING**  
BEFORE THE  
**COMMITTEE ON SMALL BUSINESS  
AND ENTREPRENEURSHIP**  
OF THE  
**UNITED STATES SENATE**  
**ONE HUNDRED EIGHTEENTH CONGRESS**  
FIRST SESSION

—————  
AUGUST 15, 2023  
—————

Printed for the use of the Committee on Small Business and Entrepreneurship



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE  
WASHINGTON : 2024

COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP  
ONE HUNDRED EIGHTEENTH CONGRESS

---

BENJAMIN L. CARDIN, Maryland, *Chairman*  
JONI ERNST, Iowa, *Ranking Member*

MARIA CANTWELL, Washington  
JEANNE SHAHEEN, New Hampshire  
EDWARD J. MARKEY, Massachusetts  
CORY A. BOOKER, New Jersey  
CHRISTOPHER A. COONS, Delaware  
MAZIE HIRONO, Hawaii  
TAMMY DUCKWORTH, Illinois  
JACKY ROSEN, Nevada  
JOHN HICKENLOOPER, Colorado

MARCO RUBIO, Florida  
JAMES E. RISCH, Idaho  
RAND PAUL, Kentucky  
TIM SCOTT, South Carolina  
TODD YOUNG, Indiana  
JOHN KENNEDY, Louisiana  
JOSH HAWLEY, Missouri  
TED BUDD, North Carolina

SEAN MOORE, *Democratic Staff Director*  
MEREDITH WEST, *Republican Staff Director*

# CONTENTS

AUGUST 15, 2023

## OPENING STATEMENTS

Page

### WITNESSES

John Hickenlooper, U.S. Senator from Colorado .....	00
Mr. Kevin Stine, Chief of the Applied Cybersecurity Division, National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, MD .....	00
Prepared Statement .....	00
Ms. Gretchen Bliss, Director of Cybersecurity Programs, Cybersecurity Programs Office, University of Colorado, Colorado Springs, Colorado Springs, CO .....	00
Prepared Statement .....	00
Mr. Alfred Ortiz, CEO, CSD Cyber, Colorado Springs, CO .....	00
Prepared Statement .....	00
Dr. Shawn P. Murray, President-Elect, International Board of Directors, Information Systems Security Association, Colorado Springs, CO .....	00
Prepared Statement .....	00



# **CYBERSECURITY: CHALLENGES AND OPPORTUNITIES FOR SMALL BUSINESSES**

**TUESDAY, AUGUST 15, 2023**

UNITED STATES SENATE,  
COMMITTEE ON SMALL BUSINESS  
AND ENTREPRENEURSHIP,  
*Washington, DC.*

The committee met, pursuant to notice, at 2:30 p.m. MDT, at UCCS Cybersecurity Center, 3650 N. Nevada Avenue, Colorado Springs, Colorado, Hon. John Hickenlooper presiding.

Present: Senator Hickenlooper [presiding].

## **OPENING STATEMENT OF SENATOR HICKENLOOPER**

Senator HICKENLOOPER. I call this meeting of the Committee on Small Business and Entrepreneurship to order. Today we are going to have a Senate Small Business Committee field hearing on the importance of cybersecurity, especially for small businesses.

We want to give special thanks to the University of Colorado at Colorado Springs, the Space Information Sharing and Analysis Center, the ISAC, and the National Cybersecurity Center for their hard work on these critical issues and for providing such a wonderful space for us to talk about space. Also thanks to Chair Cardin and Ranking Member Ernst for the opportunity to chair this hearing, for their partnership on working on these critical issues. And although they are not here personally they are here in spirit.

And especially important in light of the Air Force's decision to permanently locate Space Command here. Colorado Springs has both the small business base and local expertise to support the work of Space Command, and we look forward to a long, continued alliance with Space Command.

We are here today to focus on how to help these small businesses to thrive in an ever-changing economy, especially one where cybersecurity becomes a larger and larger risk. The changing nature of commerce means small businesses have the opportunity to integrate technology to help them grow and innovate. Internet transactions contribute roughly \$10 trillion annual to the global economy. But as technology becomes more critical to business operations, cybercrime becomes increasingly threatening. Bad actors target small businesses, large businesses indiscriminately. Sometimes they just attack anything that moves.

Sixty-six percent of all small businesses have experienced a cyberattack of some sort in the past year. These cyberattacks include software designed to harm computer systems, phishing emails, Trojan Horses that contain malware, holding data and ap-

plications for ransom. That includes weaknesses such as weak passwords that can be easily guessed or construed by bad actors.

Small businesses often, on account of their size, so often lack the resources and expertise to prevent the cyberattacks before they happen, and in many cases struggle to respond after the attack occurs. In so many cases they cannot afford to have a department or even a dedicated engineer to help them be prepared and to help guide them when they have been attacked.

Small contractors may struggle to comply with complex Federal contracting requirements. We need to make sure that with the complex systems that the Federal Government requires that we prioritize security without leaving small contractors behind. Certainly when small businesses turn to the insurance market for cyber insurance it can be challenging to understand how the policies work, how insurance can help them recover after a cyberattack, and what the value proposition is, what they are paying for, whether they are getting a fair value for their insurance.

Our bipartisan Insure Cybersecurity Act, with Senator Capito from West Virginia, is going to help provide both clarity and guidance for small businesses looking to get insured. This is an issue across industries. Even former brewpub owners are sensitive to the need to protect websites, payments, business accounts.

The Federal Government has a broad variety of programs to connect small businesses with the support they need to do business, and especially do business in this digital economy. The SBA Small Business Development Centers support small firms in a variety of ways, including cyber. One new law requires SBDCs to have employees certified cyber strategy counseling for small businesses. That means that there are answers at hand at almost all times.

A few of our witnesses today have done extensive work with the Colorado SBDC to support training small firms in this room. The National Institute of Standards and Technology, more fondly known as NIST to most of us, is a global leader—and I mean that sincerely, a global leader—in setting standards and issuing detailed guidance on privacy, connected devices, cybersecurity. We are lucky to have these deep technical experts working to protect public and private institutions, not just nationwide but globally. They establish a common language, and such a commonality of language is essential to be successful in our defense from intruders. We are excited to hear today from NIST about their work on these issues.

This is, without question, a bipartisan issue. There should be no politics involved in this in any way. I think everyone agrees that we need to expand our cyber workforce. Right now we are filling up less than 70 percent of the jobs that need to be filled, the available cyber jobs. We need to provide support, and not just support but genuine technical assistance to small businesses. At the same time, we have to raise awareness of the information that is available for cyber defense, where they can turn. And we have to, at least to some minimum level, establish these cyber standards around creating safeguards.

As our economy continues to grow and continues to digitize, we need to ensure businesses have the ability to protect themselves in cyberspace. Most important for my job here right now is to thank

all of you for being here, our witnesses. I will introduce Kevin Stine here in a moment.

Having a standard Senate hearing proceeding, or not being able to have a standard Senate hearing in the old traditional sense means we will not be taking—let's get that right. Using the standard Senate hearing proceedings means we cannot take questions from the audience, but if someone wants to sign them out to me I will do the best I can. But certainly if call, send us an email, write us a letter, we will respond and answer any questions that are asked.

We have some excellent witnesses today, and I am going to read a description of all four witnesses, although we are going to start with Kevin Stine here, who is Chief of the Applied Cybersecurity Division at the National Institute of Standards and Technology, NIST, the Information Technology Laboratory, or should I say NIST's Information Technology Laboratory. Do not get me started on the acronyms in the Federal Government.

In this role, Kevin leads NIST's collaborations with industry, with academia, and, of course, with government to improve cybersecurity and privacy risk management.

We are going to hear in a moment from Gretchen Bliss, who is the Director of Cybersecurity Programs at the University of Colorado, Colorado Springs. Gretchen has over 30 years of experience in cybersecurity and leads UCCS's academic and research efforts in cybersecurity.

Alfred Ortiz is the CEO of CSD Cyber. Alfred established his small business after over 20 years of working in cyber systems and is capable of translating even this indecipherable technology into Spanish.

Also we have Dr. Shawn Murray, President-Elect of the Information Systems Security Association. Dr. Murray is a small business owner, the incoming President of an association of IT security professionals.

So again, we are grateful to have all of you here, especially to those of you who are going to have to step up to the witness stand and bear witness.

Anyway, we will start with our first panelist, Kevin Stine, and now I will turn it over to you for your opening remarks, and then we will begin the heated questioning, well, lukewarm questioning.

**STATEMENT OF KEVIN STINE, CHIEF OF THE APPLIED CYBERSECURITY DIVISION, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE, GAITHERSBURG, MD**

Mr. STINE. I look forward to it. Perfect.

Well, thank you Senator Hickenlooper for including NIST in today's field hearing on such an important topic and here in beautiful Colorado Springs. As you mentioned, I am Kevin Stine. I am the Chief of the Applied Cybersecurity Division within the Information Technology Lab at the Department of Commerce's National Institute of Standards and Technology. Keeping track of acronyms, that is DOC NIST ITL ACD, but we will not go there.

Thank you again for the opportunity to be here today to discuss NIST's role in helping small businesses to improve their cybersecurity.

NIST has worked in the cybersecurity space since about 1972, and really prides itself on our strong partnerships with government agencies, with companies of all sizes, with academic, nonprofit entities, to really develop and improve our cybersecurity resources to best meet their needs. Our direct connections with companies and other users of our guidance helps those organizations but it also advances our efforts to inform government and private sector cybersecurity-related policy decisions.

I think as you said very clearly, cybersecurity is a challenge for all organizations, and the risks and technologies are constantly changing, and it can be difficult for any organization to keep pace. Small businesses, though, are more innovative, agile, and productive than ever thanks to the capabilities delivered by technology, but the cybersecurity challenges for small businesses certainly loom larger than ever.

Not every small business is the same. Their risks will vary. So whether you are a small coffee shop or a brewpub, your risks could be very different compared to a small company that maintains millions of health records, for example.

At NIST we believe in risk-based approaches to ensure organizations have the tools to address their specific needs. We have a long-standing effort to help small companies meet their cybersecurity needs. In response to the NIST Small Business Cybersecurity Act several years ago we launched the NIST Small Business Cybersecurity Corner to help put key resources in one place. The Small Business Administration, the Department of Homeland Security, the Federal Trade Commission, and others have contributed resources to that NIST site, and they are also providing small business-focused resources to be shared through our site, and they promote its awareness and use.

In March of this year, NIST launched a Small Business Cybersecurity Community of Interest to convene companies, trade associations, and others who can share business insights, expertise, challenges, and perspective to guide our work and assist NIST to better meet the cybersecurity needs of small businesses. Members of this community are learning about NIST's current and planned resources intended for smaller organizations, and they also provide us with on-the-ground feedback about the usefulness of those resources and how to approve them.

Beginning in 2013, NIST created the Framework for Improving Critical Infrastructure Cybersecurity, which is commonly referred to as the Cybersecurity Framework or the CSF, which many organizations, including many small businesses, use to better understand, communicate, and reduce cybersecurity risk.

Just last week, on August 8th, we issued a complete redraft of the Framework for public comment, and we have based our proposed update on lessons learned from the use of the Framework over the last several years. CSF 2.0, as we call it, is explicitly intended to be used by organizations of any size and in any sector. We have been hosting workshops and collecting comments to inform improvements to the framework, and that includes reaching

out to small businesses for their perspectives, which has been very valuable.

Small manufacturers also represent a critically important part of the community. The mission of NIST Manufacturing Extension Partnership, or the MEP, is to assist small and medium-sized manufacturers. MEP operates a nationwide network, with centers in every state and in Puerto Rico, and through this program NIST partners with others to provide awareness, training, and hands-on cybersecurity assistance to smaller manufacturers to help them secure their business information and assets.

You mentioned cybersecurity workforce in your opening remarks. A skilled and diverse cybersecurity workforce in organizations, including, and sometimes especially in smaller companies, is critical to improving the nation's cybersecurity capabilities. Another program led by NIST is NICE—I do not always pick the acronyms, but it is a nice one—which enhances cybersecurity education, training, and workforce development capabilities of the United States. Through NICE we have produced tools and provide resources to help large and small organizations alike to understand and address their cybersecurity workforce needs.

We are also home to the National Cybersecurity Center of Excellence, which is a collaborative hub where industry, government agencies, and academic institutions and others work together to address cybersecurity challenges facing U.S. businesses of all sizes.

And while we have developed cybersecurity guidance and other resources for small businesses, we are also focused on increasing the security of the technology that we all leverage each and every day, including, for example, our work on next-generation encryption and our efforts to secure software platforms, networks, and connected devices.

So again, thank you for the opportunity to explain NIST's cybersecurity portfolio and how it applies to a wide variety of users, from small and medium-sized enterprises to large, private and public organizations. We know how real and difficult the challenges are, and it is part of our job to help organizations of any size, in any sector, to successfully tackle those challenges so they can do their jobs better.

So thank you again for including us, and I look forward to any questions you might have.

[The prepared statement of Mr. Stine follows:]



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)<sup>1</sup>, 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.

---

<sup>1</sup> 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<sup>2</sup>. Small businesses accounted for 62.7% of net jobs created from 1995-2021<sup>3</sup>.

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

---

<sup>2</sup> <https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/>

<sup>3</sup> <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<sup>4</sup> puts these key resources in one place.

Congress has given NIST responsibility<sup>5</sup> 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.

---

<sup>4</sup> <https://www.nist.gov/itl/smallbusinesscyber>

<sup>5</sup> <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<sup>6</sup>, 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**

---

<sup>6</sup> <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<sup>7</sup> 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<sup>8</sup>, 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

---

<sup>7</sup> <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

<sup>8</sup> <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.



Senator HICKENLOOPER. You bet. Thank you, Kevin, and I appreciate you taking the time out of your busy schedule to get over here for this hearing.

Obviously, you are concerned with cyber in all dimensions. How do you think about cyber within small businesses, specifically, and in what ways do you try to think of that, you know, communicate to that community in a specific way?

Mr. STINE. Yeah. Cybersecurity, at times, has its own language that we speak, so it is important to be able to talk about cybersecurity in a way that will be more consumable and digestible to organizations of all shapes and sizes across all different sectors, and that certainly is inclusive of small businesses.

Tools like the Cybersecurity Framework provide, in our view, a common language or a common taxonomy that is intended to help break down some of those communications divides both within companies but also across companies and across sectors, and even across nations as well. We think there is a lot of value in having a common language that is provided by the Cybersecurity Framework.

Senator HICKENLOOPER. What are some of the key pieces of feedback that you have received from NIST's new Small Business Cybersecurity Community of Interest?

Mr. STINE. The Small Business Cybersecurity Community of Interest. We take small business cybersecurity very seriously, and it is certainly woven into all parts of our cybersecurity and our privacy portfolio at NIST. We stood up the Community of Interest just a few months ago to really help drive more involvement, and I would say that is bidirectional involvement with the small business community, both the businesses themselves but also their advocates. It could be associations. It could be service providers to small businesses, for example. And we think having that open line of communication, that bidirectional communication is tremendously valuable for us to help share updates with the small business community on things we are working on but also receive feedback directly from them.

And I think over the last few months there are a few themes that I think we have heard in these formative months. The first, I think there has been overwhelming appreciation for having a venue like the Small Business Cybersecurity Community of Interest, where different players in the community can get together, share their experiences, and certainly communicate directly with NIST.

We frequently hear that one of the big challenges for small businesses, because cybersecurity can be overwhelming, and certainly the standards and guidelines can be overwhelming as well, just the sheer volume of those resources alone can be overwhelming. So being able to discuss just simply where to start—Where do I start? What are some resources that I should start with as a small business to really get a better sense of where I am today from a cybersecurity perspective and where I might need to be, and what are some potentially quick steps I can take on my journey? So hearing that has been very helpful.

And I think the final piece that we have heard, and the final theme, would be the need and the importance for tailored resources. Again, we produce a lot of standards and guidelines and

other agencies and other organizations, public and private, produce resources for small businesses. And not all of those resources are written in a way that are tailored or customizable for the unique needs of small businesses.

So the learnings that we are kind of observing early on is just the validation that as we are producing standards and guidelines, as we are producing other resources to be able to reflect those to the small business community and get their feedback early and often so that the things that we produce are going to be the most useful and digestible for them.

Senator HICKENLOOPER. Integrate it. Take that feedback into the policy.

Last week, NIST released a new draft of their highly regarded Cybersecurity Framework, as you were describing, after beginning the 2.0. I know that the NIST Cybersecurity Framework was well received by many large companies. What has the response been—I am sure you have a broader range of responses, but what has the overall response been from the small business community?

Mr. STINE. We have been thrilled with the uptake of the Framework since we first issued it in 2014, and certainly we have seen tremendous growth and increased uptake across all sectors and all sizes of organizations since we issued that first version back in 2014. And that includes small businesses, and we have had many small businesses that have been on the Cybersecurity Framework journey with us since the early days and have become great advocates and amplifying voices for the use of the Framework for small businesses.

But I think this 2.0 update process provides us a great opportunity to kind of reevaluate the Framework, reevaluate its utility for small businesses, and I would say more importantly, or just as importantly, the types of derivative resources we can produce to really help make it more consumable and digestible for small organizations.

I think that common language that it provides is probably the greatest value provision, if you will, for the framework, because it can speak to and be understood by non-cybersecurity, non-technical folks, maybe the folks that understand mission and risk, maybe not cybersecurity risk, but they understand risk, and being able to talk about cybersecurity risk in that bigger enterprise risk discussion, whether your enterprise is 10 people in a coffee shop or a brewpub, or a much larger multinational organization. We think there is a lot of value in that, and we are excited to continue to get feedback during this draft comment period to help further inform the framework.

Senator HICKENLOOPER. And I have not seen this in previous discussions. That common language, I agree with you, is crucial. In a funny way it almost allows you to be able to measure and begin to define increments of measure, which allows one to create not only defenses but solutions when you have been hacked.

How does that integrate? In other words, are you trying to figure out the increments of measure by which you could classify attacks as part of this overall language that is being created?

Mr. STINE. Measurement is a challenging area in the cybersecurity space, especially for a precision measurement organization like

NIST. I do not know that you are going to get down to the next—best—

Senator HICKENLOOPER. Atomic clocks.

Mr. STINE. Yeah. We do have that, and that is a very precise measurement and a lot of value there. Cybersecurity is a different beast at times. But certainly there are things that you can measure today.

But I think the value, again, of the Cybersecurity Framework, again, that common language and taxonomy is bringing in a whole different set of users to the cybersecurity discussion, which is tremendously valuable. It is not just the technologists and the cybersecurity professionals. It is the educators. It is the lawyers. It is the human resources professionals. And I think as more folks, kind of that “big tent” approach, as more folks become part of that tent and that community there are going to be new and innovative ways to not only use the Framework but also the technologies and the services and the approaches to help achieve those outcomes that are expressed in the framework. We are going to learn a lot about that and help improve future versions as well.

Senator HICKENLOOPER. I think that is one of the amazing things about NIST. Again, the United States is home to a center. I mean, most of us in business learned early on that what gets measured is what is gets done. If you cannot measure things you are going to have a hard time achieving results. And yet in something like this it is growing at a rate that makes it almost impossible to have a common language, let alone to measure the different things. That framework of language you are creating is actually going to allow—it is a little bit the same thing with fighting climate change, that we do not have the capability to measure accurately climate-changing emissions at the level at the level it needs to be done to really address it. But NIST will figure that out as well.

Mr. STINE. We are on it.

Senator HICKENLOOPER. I am not trying to alarm anybody. I just want to make sure that they feel secure in NIST’s mission.

What other guidance do you think small businesses need in order to deal with some of these cybersecurity risks?

Mr. STINE. There are a lot of standards and guidelines that exist today in the cybersecurity and increasingly the privacy space. Certainly we produce a lot of those. Others produce them as well. But I think, again, what we have heard very clearly from the small business community and those that provide services to support them are taking the voluminous guidance that might exist today and really distilling it down into much more practical, actionable, and consumable resources, things like Quick Start guides, templates, fact sheets, those types of things that can distill the sometimes very complex and potentially technical information into something that is going to be a little bit more immediately actionable.

And again, I used the phrase earlier, organizations are on the journey. And as small businesses start on that journey and they begin to improve there are certainly more robust resources that can help them advance their cybersecurity capabilities.

Senator HICKENLOOPER. And think that journey, there is a microcosm going on 100 times or 1,000 times in any company. Each indi-

vidual is going on that journey, and I think you are exactly right to be able to find those increments of information so that they can get on board and get engaged and grow into the complexity of the subject and hopefully help create those increments of measure as we go down the road.

Obviously, just extending that train of thought, small businesses are part of a larger food chain, as it were. Maybe that is an inappropriate word, but let's call it a supply chain, to stay with a more acceptable business nomenclature. Obviously, the smaller firms are vital parts of the supply chains that bigger companies count on, and we have seen this frequently since the pandemic, that when these supply chains get interrupted it disrupts our entire economy.

What is NIST doing to help secure or make more secure these complex supply chains that integrate small, medium, and large businesses?

Mr. STINE. Yeah, you are absolutely right, and this is such a critical topic for so many organizations. We have a longstanding program, an area of focus on cybersecurity supply chain risk management, so helping organizations better understand and manage the cybersecurity risks in the context of their supply chain activities. We certainly have produced guidance and different types of best practices that we have kind of gleaned from the best practices of other organizations over the years to really help organizations, again, of all shapes and sizes across all different sectors, but particular small business, to better understand and then manage their cybersecurity risks in the context of supply chains.

You know, every organization, large or small, is either a producer of technologies or services but also a consumer of those same services. So I think one of the frequent pieces of feedback we provide to small businesses, and certainly even large businesses as well, as they are interacting with smalls, is understanding and having more visibility into your supply chains, understanding what you are providing, what the expectations are from you, and then being able to clearly express what those capabilities are from a cybersecurity perspective.

I think increasingly we are also trying to take the standards and guidance and other technologies and practices that exist today and begin to demonstrate very practical example implementations of those, in the supply chain space in particular, through our National Cybersecurity Center of Excellence to provide, in some cases, some blueprints and some worked examples that can give really any organization, but I think increasingly small businesses a better starting place on this journey as well.

Senator HICKENLOOPER. Right. Michael, are we out of time? What is your sense of this, for the first panel. We are good? So I can ask another question. Good. Check with John Conrad because I do not really trust you, Michael. No, I am just kidding. I am just kidding. [Laughter.]

Senator HICKENLOOPER. It is all about security. It is all about security.

You were saying this, that so many small businesses lack the time and the money and the personnel to really address cybersecurity and to assess what is necessary and the resources to create security. But if they could be provided the essential information, in

a compact way, as you say, I think you used the word “digestible,” easily digestible, small businesses, I think, would make consistently better decisions.

Is NIST able to coordinate, or are you already coordinating and partnering with other agencies in the Federal Government, such as the SBA here today, to ensure that small businesses are getting accurate, the right information, to be prepared for threats and to be able to respond?

Mr. STINE. We do work very closely with our interagency partners and increasingly other organizations outside the Federal Government as well, and I think through programs like the Small Business Cybersecurity Corner as well as the Community of Interest that we just established, we think those are going to be very helpful mechanisms as well to share resources from different parts of the interagency, whether it is SBA, or the Federal Trade Commission, our colleagues at the Department of Homeland Security, and CISA in particular, and many others.

So there are a lot of opportunities for us to coordinate and collaborate across the interagency to bring those resources to bear. And we do the same with many of our public sector or non-government entities. For example, the National Cybersecurity Alliance is another great resource that we work very closely with to help amplify their message, and vice versa.

We think there are plenty of resources. There are a lot of resources. There are a lot of coordination opportunities, and we are happy to coordinate and engage and play our part.

Senator HICKENLOOPER. And are you able to focus on some of the networks that are smaller but make up the constituency that the SBA services, say women-owned or minority-owned businesses?

Mr. STINE. We are, and I think that is where some of the opportunities working with even other commerce bureaus. Like the Minority Business Development Agency, for example, within the Department of Commerce, or within NIST’s Manufacturing Extension Partnership are two great mechanisms that have nationwide networks and tentacles out there, if you will, to help reach diverse communities, including minority- and women-owned businesses. So tremendous value there.

And I think part of the opportunity we have with the Cybersecurity Framework 2.0 update process is we really need to double down in our engagement with more diverse parts of the community to get their unique feedback to help inform the framework so that it can be the most useful for all involved.

Senator HICKENLOOPER. Right. Last question, and I appreciate that. Obviously, companies large and small have to worry about cybersecurity, as you have been explaining, but also concerns about privacy, and different but similar, protecting the information of their customers. These three issues kind of intersect in small firms especially. So how do you help them address all three of these concerns as efficiently as possible?

Mr. STINE. One of the most exciting parts and areas of most significant growth in our broader program in NIST is our Privacy Program. We think there is just tremendous opportunity there, both from the privacy risk management perspective but also the privacy-

enhancing technologies perspective. There are a lot of very exciting and innovative approaches that are out there.

We try to ensure that for all the potential points of integration between cybersecurity and privacy, and there are many, many cybersecurity standards and controls and capabilities help to improve privacy protections as well, and that goes in both directions. So we try to take every advantage of the relationships and the expertise we have and the relationships we have in the community to highlight those points of intersection and really work with the innovators in the community to be able to produce the technologies and the resources that can be most useful.

Senator HICKENLOOPER. Right. Absolutely. Well, I hate to interrupt this but I look forward to continuing the conversations over a cold beer at some point, to talk about something we do know how to measure properly.

Mr. STINE. Yes, we do. We do that as well.

Senator HICKENLOOPER. Anyway, thank you so much for your public service and investing so much of your life into something that is clearly tremendously important to the country, but I think underappreciated by most of the public. So that is always when public service is at its most public that you have to go on the line day in and day out and provide answers to difficult questions, and the public not really appreciating what you do. I think over the next few years the public will more and more appreciate people like yourself that are really working so hard to keep us safe. So thank you very much.

Mr. STINE. Thank you, sir. I appreciate it.

[Applause.]

[Break.]

Senator HICKENLOOPER. The only places you see such a rapid change of sets is in Hollywood or Washington, D.C., but here we are matching them in time.

I want to welcome back, although you really have not gone anywhere, but welcome back from the front row Gretchen Bliss, Alfred Ortiz, and Dr. Shawn Murphy—Murray. One of my oldest friends is named Shawn Murphy, and I am probably going to do that three or four times over the course of the next hour.

Anyway, Gretchen is the Director of Cybersecurity Programs at the University of Colorado, Colorado Springs, which we mentioned earlier, Alfred Ortiz is the CEO of CSD Cyber, and Dr. Murray is the President-Elect of the Information Systems Security Association.

[Applause.]

Senator HICKENLOOPER. That was a better plug than I thought.

All right. First a question that you can each do in turn. Gretchen, we will start with you and just work down the line. Obviously, cybersecurity is a bipartisan issue. It requires a whole-of-government approach both to assessing the risk and trying to be able to preempt the cyber threats that we know are out there. And I appreciate all of you being here.

What is the number one issue each of you would recommend we highlight as we work with the executive branch on ways to help small businesses safeguard their data? You are all experts.

Oh, what am I saying? You are supposed to do introductory statements and I went right to the questions. I get excited. What can I say? I apologize. We will go and let each of you do your opening statements, please.

**STATEMENT OF GRETCHEN BLISS, DIRECTOR OF CYBERSECURITY PROGRAMS, CYBERSECURITY PROGRAMS OFFICE, UNIVERSITY OF COLORADO, COLORADO SPRINGS, CO**

Ms. BLISS. Thank you so much. As the Senator mentioned, I am Gretchen Bliss. I am the Director of Cybersecurity Programs at the University of Colorado, Colorado Springs. I am very honored to be here, to be invited to discuss my thoughts and background in bringing cybersecurity, small business, education, and students together to raise the bar on cybersecurity for all.

The Colorado Springs ecosystem has been developing for at least the last 9 years into a coalition of the willing that connects education, industry, government, and community. The workforce demand for cybersecurity professionals is huge. Over 663,000 jobs are available today across the nation, 22,641 of those in Colorado alone.

Cybersecurity is needed across all industry sectors, not just for military or government contractors, agencies, and departments. The National Cybersecurity Workforce and Education Strategy that was recently released, stated that, "Responsibility for defending cyberspace should be shifted from individuals and small businesses to the most capable actors in cyberspace, and vigorous collaboration among education, labor, and commercial stakeholders is essential to success."

Small Businesses face mounting and expanding challenges regarding cybersecurity protection and threats. To underscore the need, Forbes reports that in 2021 alone, 70 percent of ransomware attacks were directed at small and mid-sized businesses.

We are currently leveraging several federally funded initiatives to support collaboration among education and small business. Years back, our Pikes Peak State College team received a Regional Alliances and Multistakeholder Partnerships to Stimulate—RAMPS, another great acronym—grant from NIST's NICE, since Kevin already covered that. We built the Cyber Prep program, where 17 high school students in the summer were paired with 14 small businesses, some of them sitting at this table, and they had a paid internship and got cybersecurity training sessions. The businesses were shocked at the depth of talent that high school students possessed in cybersecurity. Two of the students have continued with their companies through college and beyond.

Of the over 400 U.S. institutions that the National Security Agency has designated as Centers of Academic Excellence in Cybersecurity, 15 are in the state of Colorado. UCCS was the first CU system school designated as a Center of Academic Excellence in 2012. The CAE program helps to standardize academic cybersecurity programs. It provides grants to support the expansion and collaboration between these educational programs across the country.

Government and industry demand three things from a community student: a degree, industry-recognized certification, and hands-on experience. The grants that the CAE has provided provide stu-

dents with that experience and knowledge they need to be later hired to support cybersecurity needs across industry.

Regionally, education and small business collaborate through the Small Business Development Center programs. One called Cyber Cover Your Assets, CYA, and the annual Colorado SBDC Network Cybersecurity conference. This program was the first of its kind and is leading programs nationwide. Small businesses work with the SBDC under an 8-week cyber implementation program where they receive risk assessment and education and budget-friendly solutions to secure their business assets. In addition, community experts, small businesses—represented by my co-panelist Shawn Murray—and high school and community college students conduct cybersecurity hygiene checkups for small businesses.

We actually just found out late last night that the collaboration between the SBDC, who is represented here, UCCS, NCC, and Murray Security Services were awarded a \$1 million grant from SBA to bring cyber clinics, not unlike legal and medical clinics, to students and small businesses to build resilience and collaboration to solve those cybersecurity challenges.

[Applause.]

Ms. BLISS. Research is also fundamental to bringing businesses, government, and students together to solve those wicked-hard problems in cybersecurity. UCCS has a robust cybersecurity faculty that was awarded over \$19 million in government funds over the past 3 years to conduct in-depth research for the Department of Defense, Department of Energy, the National Science Foundation, Cyber Command, Space Command, and industry partners. Research not only solves complex problems but also prepares students for industries' workforce needs. Continued research funding across government agencies remains critical to solving these problems.

The Space Information Sharing and Analysis Center, ISAC, is an embedded partner with UCCS, over in our other building here, and they have over 70 small, medium- and large-sized companies as members. The Space ISAC facilitates collaboration against cyber and space threats across the global space industry, enhancing industry preparation for, and in response to, vulnerabilities, incidents, and threats. It also hosts a fellowship program for industry and educational fellows. Cross-disciplinary organizations, such as the Space ISAC, develop cyberspace resiliency throughout industry, government, and education.

UCCS is leading the University of Colorado system and the state in finding new and unique ways to create cybersecurity partnerships with small businesses. UCCS has developed a workforce pipeline that begins in K-12 and crosses into community colleges and the CU system to ensure cyber capabilities are available to Colorado at many levels. Over the past four years, UCCS has expanded cybersecurity degrees and programs to 20 pathways across five colleges, beyond the longstanding cornerstone programs in our engineering department at the bachelor's, master's and doctorate levels.

Programs can now be found in the College of Public Service with a cyber law, policy, and forensics concentration; our Letters Arts and Sciences with a Technical Communication and Information Design bachelor's degree; our College of Business with Cybersecurity Management degree at the bachelor's, MBA, and DBA levels; and

finally, the College of Education, where we do teacher prep workshops to bring cybersecurity into the classroom to make teachers comfortable and share it with their students down to the middle school level. Needless to say, UCCS believes strongly in cybersecurity as an interdisciplinary necessity.

The nation benefits greatly from community programs such as those at UCCS, NIST, NICE, CAE, Space ISAC, Colorado Springs Community and SBDC. These programs develop a workforce so direly needed to protect our national security and solve those hard technical problems for the country. They bring small businesses together with education to create the future workforce that will solve complex problems and raise the bar for cybersecurity nationwide.

[The prepared statement of Ms. Bliss follows:]

Statement by Gretchen Bliss, UCCS Director of Cybersecurity Programs

Senate Small Business Committee

15 August 2023

UCCS Kevin W. O'Neil Cybersecurity Education and Research Center

I am Gretchen Bliss, Director of Cybersecurity Programs at the University of Colorado at Colorado Springs (UCCS). I am honored to be invited to discuss my thoughts and background in bringing cybersecurity, small business, education, and students together to raise the bar in cybersecurity for all.

The Colorado Springs ecosystem has been developing for the last nine years into a coalition of the willing that connects education, industry, government, and community. The workforce demand for cybersecurity professionals is HUGE: over 663,000 jobs are available today across the nation (22,641 in Colorado alone). Cybersecurity is needed across **all** industry sectors, not just for military or government contractors, agencies, and departments. The National Cybersecurity Workforce and Education Strategy recently stated, "Responsibility for defending cyberspace should be shifted from individuals and small businesses to the most capable actors in cyberspace, and vigorous collaboration among education, labor, and commercial stakeholders is essential to success." Small Businesses face mounting and expanding challenges regarding cybersecurity protection and threats. To underscore the need, Forbes reports that in 2021, [70% of ransomware attacks](#) were directed at small- and mid-sized businesses.

We are currently leveraging several federally funded initiatives to support collaboration among education and small business. Years back, our Pikes Peak State College team received a Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) grant from NIST's National Initiative of Cybersecurity Education (NICE). We built the Cyber Prep program, where 17 high school students were paired with 14 small businesses in Colorado Springs for a summer paid internship and cybersecurity training sessions. Businesses were shocked at the depth of talent that high school students possessed in cybersecurity; two students continued with their companies through college and beyond.

Of the over 400 US institutions that the National Security Agency designates as Centers of Academic Excellence (CAE) in Cybersecurity, 15 are in Colorado. UCCS was the first CU system school designated as a CAE in 2012. The CAE program helps to standardize academic cybersecurity programs. It provides grants to support educational programs that develop cyber clinics, like legal and medical clinics, where students get practical hands-on experience helping small businesses. Industry demands three things from a cybersecurity student: a degree, industry-recognized certifications, and hands-on experience. Clinics give students the experience and knowledge they need to be later hired to support cybersecurity needs across industries.

Regionally, education and small businesses collaborate through Small Business Development Center (SBDC) programs called Cyber Cover Your Assets (CYA) and the annual Colorado SBDC Network Cybersecurity conference. This program was the first of its kind and is a leading program nationwide. Small businesses work with the SBDC under the 8-week cyber implementation program where they receive a risk assessment and education- and budget-friendly solutions to secure their business assets. In addition, community experts, small businesses -- represented by my co-panelist Shawn Murray -- and

high school and community college students conduct cybersecurity hygiene checkups for small businesses. Senate funding for these initiatives will support their proliferation across the country.

Research is also fundamental to bringing businesses, government, and students together to solve the wicked-hard problems in cybersecurity. UCCS has a robust cybersecurity faculty that was awarded over \$19M in government funds over the past three years to conduct in-depth research for the DoD, DoE, NSF, CyberCOM, SpaceCOM, and industry. Research not only solves complex problems; but also, prepares students for industries' workforce needs. Continued research funding across government agencies remains critical.

The Space Information Sharing and Analysis Center (ISAC) is an embedded partner with UCCS and has over 70 small, medium- and large-sized companies as members. The Space ISAC facilitates collaboration against cyber and space threats across the global space industry, enhancing industry preparation for -- and response to -- vulnerabilities, incidents, and threats. It also hosts a fellowship program for industry and educational fellows. Cross-disciplinary organizations, such as the Space ISAC, develop cyberspace resiliency throughout industry, government, and education.

UCCS is leading the University of Colorado system and the state in finding new and unique ways to create cybersecurity partnerships with small businesses. UCCS has developed a workforce pipeline that begins in K-12 and crosses into community colleges and the CU system to ensure cyber capabilities are available to Colorado at many levels. Over the past four years, UCCS has expanded cybersecurity degrees and programs to 20 pathways across five colleges, beyond the long-standing cornerstone programs in engineering at the bachelor's, masters and doctorate levels. Programs can now be found in the College of Public Service with a cyber law, policy, and forensics concentration; Letters Arts and Sciences with a Technical Communication and Information Design Degree; College of Business with Cybersecurity Management at the BS, MBA, and DBA levels, and College of Education teacher prep workshops to bring cybersecurity into the classroom. Needless to say, UCCS believes strongly in cybersecurity as an interdisciplinary necessity.

The Nation benefits greatly from community programs such as those at UCCS, NIST and NICE, CAE, Space ISAC, and SBDC. These programs develop a workforce so direly needed to protect our national security and solve hard technical problems for the country. They bring small businesses together with education to create the future workforce that will solve complex problems and raise the bar for cybersecurity nationwide.

Links to referenced programs:

Cyberseek heatmap: <https://www.cyberseek.org/heatmap.html>

RAMPS Program: <https://www.nist.gov/itl/applied-cybersecurity/nice/ramps-communities>

CAE Community: <https://www.caecommunity.org/>

Pikes Peak SBDC CYA: <https://pikespeaksbdc.org/what-we-do/programs/sbdc-techsource-cyber-cya/>

Space ISAC: <https://s-isac.org/>

UCCS Cybersecurity: <https://cybersecurity.uccs.edu/>

UCCS research:

## UCCS Cybersecurity Expertise

Policy/Law-maker    DoD Commander    CEO/CTO/CSO/CIO

<b>Public Policies, Laws, Governance, Ethics, Compliance</b>			
<b>Quantitative, Trustworthy, Autonomous, and Agile (QTAA) Decision-Making (e.g., for Command and Control)</b>			
<b>Cybersecurity Metrics and Quantification</b>			
<b>Trustworthy Sensing/Intelligence (Situational Awareness)</b>			
<b>Trustworthy Artificial Intelligence/Machine Learning</b>			
<b>Resilient Architectures and Security &amp; Privacy Mechanisms</b>			
<b>Enterprise/IT networks</b>	<b>CPS/IoT/IoBT/5 &amp;6G networks</b>	<b>Critical infrastructure (Smart "X")</b>	<b>Blockchain networks</b>

Legend

**UCCS-unique & world-leading expertise**

Senator HICKENLOOPER. Thank you very much.  
Mr. Ortiz.

**STATEMENT OF ALFRED ORTIZ, CEO, CSD CYBER, COLORADO SPRINGS, CO**

Mr. ORTIZ. Good afternoon, Senator Hickenlooper, staff, and attendees. My name is Alfred Ortiz and I am the CEO of CSD Cyber, with 20 years of cyber and IT experience, moving from corporate America and starting my business over 5 years ago. As a small Colorado-based enterprise, I understand what it takes to grow a small business. In addition to CSD Cyber, I volunteer with the local Pikes Peak SBDC as a cyber expert and serve as a member of the board of directors for the local ISSA chapter. I have taught undergraduate and graduate students with a focus on cybersecurity at the University of Colorado, Denver.

I have dedicated my working career to helping individuals and firms keep their data safe from threats. My father and grandfather were entrepreneurs, so owning a small business and understanding its demands are embedded in my daily life as I work with people from all facets of our society.

Cybersecurity is an all-partisan issue that affects Americans from every strand of our society as they may be affected personally and professionally. Approximately two-thirds of American business comes from small and medium entrepreneurs, like me and many attending today, and those whose small businesses are affected by Federal legislation. Of these small enterprises, those with less than 50 employees, 47 percent of them, do not have a budget for cybersecurity. Adding to this, approximately 76 percent of SMBs, or 25.2 million businesses, have experienced a cyberattack in the last 6 months. Many will not recover. From malware, ransomware, to social engineering and other threats, small firms have more demands with the least number of resources to defend themselves.

CSD can cite circumstances where we have helped companies at all tiers. In one instance, we helped a small bank comply with Federal regulations, and a Fortune 50 company to do the same. Another time, CSD worked with a town to demonstrate the vulnerabilities of their water utility system so the residents can have safe drinking water, and we helped a local gym in securing their wireless network so their members can listen to their music safely as they work out.

At times, firms like these do not know where to go for help or are limited on resources and might not know who to trust, they may have to decide on buying that new piece of capital equipment, fly to meet a client, or spend on advertising, not thinking about securing their vital data and that of their clients.

Advocating for small business, CSD Cyber launched an SMB store on the Fourth of July this year for this very reason, to give SMBs options where they can go to for help with a reasonable price. With larger consulting firms charging over \$500 an hour, we hope to change the rules by giving small business a fighting chance. Spending on cybersecurity is a necessity for today's market, yet every firm knows that driving revenues is the lifeblood of their business.

The U.S. Federal Government is the largest buyer of goods and services in our country. With that, our small and medium businesses make up over two-thirds of our economy and should have a fair shake at the table for business.

When the CHIPS and Science Act was invoked, President Biden stated that it represents “a once-in-a-generation investment in America itself.” With approximately \$57.2 billion to be funded, one might ask, were set-asides for SMBs and minority firms placed in the legislation so larger corporations could contract and fulfil their obligations with this Federal funding?

More importantly, there needs to be considerations for small business to make it easier to participate in the Federal bidding process. When it takes 3 to 6 months to fill out a bid for an opportunity and another year to 18 months to wait for the award, many small businesses cannot sustain that cycle.

If these small enterprises do not sustain themselves with revenues and cybersecurity investment the Federal Government may have a three-fold problem: One, vital data on Americans may be lost to the dark web; two, for every SBA loan that fails, a person and their family will fall under that burden and lastly the Federal government will lose tax revenues. In short, cybersecurity is an all-American issue that affects American business.

In conclusion, I am here before you with an unwavering commitment to the pivotal realms of cybersecurity, small business prosperity, and legislative foresight. As a CEO, educator, and citizen, I come armed with a wealth of IT experience and the enduring legacy of my family’s entrepreneurial spirit.

The resonance of our dialogue today reverberates far beyond these walls, underscoring the urgency of safeguarding data in a digital age, touching every facet of American society. Through the lens of CSD Cyber’s transformative collaborations, I have witnessed firsthand the pressing need for accessible solutions that empower entities of all scales to secure their futures.

As we forge ahead into an era of legislative possibilities, let us champion the inclusion of small and minority businesses as integral contributors, fueled by equitable opportunities and streamlined processes. Together, we have the power to reshape the trajectory of our economy, bolstering its very foundation with the resilience of entrepreneurship and the fortified defense of cybersecurity.

Thank you, Senator Hickenlooper, staff, and guests. I will now hand back my time to you, Senator.

[The prepared statement of Mr. Ortiz follows:]



Cybersecurity: Challenges and Opportunities for Small Business  
 Tuesday, August 15, 2023 @ 14:30  
 National Cybersecurity Center: 3650 N. Nevada Ave., COS, CO



Statement from Alfred Ortiz  
 Time Approximately: 5m 40s

Good afternoon, Senator Hickenlooper, staff, and attendees. My name is Alfred Ortiz I am the CEO of CSD Cyber and have over 20 years of cyber and IT experience, moving from corporate America and starting up my business over five-years ago. As a small Colorado based enterprise, I understand what it takes to grow a small business. In addition to CSD Cyber, I volunteer with the local Pikes Peak Small Business Development Center as a cyber expert and serve as a member of the board of directors for the local ISSA chapter. I have taught undergraduate and graduate students with a focus on cybersecurity at the University of Colorado, Denver. I have dedicated my working career to helping individuals and firms keep their data safe from threats. My father and grandfather were entrepreneurs, so owning a small business and understanding its demands are embedded into my daily life as I work with people from all facets of our society.

Cybersecurity is an **All-Partisan** issue that affects Americans from every strand of our society as they may be affected personally and professionally. Approximately two-thirds of American business comes from small-business entrepreneurs like me and many attending today and those who's small businesses are affected by Federal legislation. Of these small enterprises, those with less than 50 employees, 47% of them have no budget for cybersecurity. Adding to this, approximately 76% of SMBs (or 25.2 million businesses) have experienced a cyber-attack in the last six months. Many will not recover. From malware, ransomware, to social engineering and other threats, small firms have more demands with the least number of resources to defend themselves.

CSD Cyber can cite circumstances where we have helped companies at all tiers. In one instance we helped a small bank comply with federal regulations, and a fortune 50 company to do the same. Another time CSD worked with a town to demonstrate the vulnerabilities of their water utility system, so the residents can have safe drinking water. And helped a local gym in securing their wireless network, so their members can listen to their music safely as they work out. At times firms like these don't know where to go for help or are limited on resources and might not know who to trust, they may have to decide on buying that new piece of capital equipment, fly to meet a client or spend on advertising, not thinking about securing their vital data and that of their clients. Advocating for small business, CSD Cyber launched an SMB store on the 4th of July for this very reason, to give SMBs options where they can go to for help with a reasonable price. With larger consulting firms charging over \$500 an hour we hope to change the rules to giving small business a fighting chance. Spending on cybersecurity is a necessity in today's market, yet every firm knows that driving revenues is the lifeblood of their business.

The US Federal Government is the largest buyer of goods and services in our country. With that, our small and medium businesses make up over two-thirds of our economy and should have a fair shake at the table for business.



Cybersecurity: Challenges and Opportunities for Small Business  
Tuesday, August 15, 2023 @ 14:30  
National Cybersecurity Center: 3650 N. Nevada Ave., COS, CO



When the CHIPS & Science Act was invoked, President Biden stated that it represents “a once-in-a-generation investment in America itself.” With approximately \$57.2 billion to be funded.

One might ask, were set asides for SMBs and minority firms placed in the legislation so larger corporations could contract and fulfil their obligations with this Federal funding?

More importantly, there needs to be considerations for small business to make it easier to participate in the federal bidding process. When it takes three to six months to fill out a bid for an opportunity and another year to 18 months to wait for the award...many small businesses cannot sustain that cycle. If these small enterprises do not sustain themselves with revenues & cybersecurity investment the Federal government has a three-fold problem: 1. Vital data on Americans may be lost to the dark web. 2. For every SBA loan that fails, a person and their family will fall under that burden and lastly the Federal government will lose tax revenues. In short, cybersecurity is an All-American issue that effects American business.

In conclusion, I am here before you with an unwavering commitment to the pivotal realms of cybersecurity, small business prosperity, and legislative foresight. As a CEO, educator, and citizen, I come armed with a wealth of IT experience and the enduring legacy of my family's entrepreneurial spirit. The resonance of our dialogue today reverberates far beyond these walls, underscoring the urgency of safeguarding data in a digital age touching every facet of American society. Through the lens of CSD Cyber's transformative collaborations, I have witnessed firsthand the pressing need for accessible solutions that empower entities of all scales to secure their futures. As we forge ahead into an era of legislative possibilities, let us champion the inclusion of small and minority businesses as integral contributors, fueled by equitable opportunities and streamlined processes. Together, we have the power to reshape the trajectory of our economy, bolstering its very foundation with the resilience of entrepreneurship and the fortified defense of cybersecurity.

Thank you, Senator Hickenlooper, staff, and guests.

I will now hand back my time to the moderator.

Senator HICKENLOOPER. Thank you. Thank you, Alfred.  
Dr. Murray.

**STATEMENT OF SHAWN P. MURRAY, Ph.D., PRESIDENT-ELECT,  
INTERNATIONAL BOARD OF DIRECTORS, INFORMATION SYS-  
TEMS SECURITY ASSOCIATION, COLORADO SPRINGS, CO**

Mr. MURRAY. Thank you, Senator. As mentioned, my name is Shawn Murray. I am the President and Chief Academic Officer at Murray Security Services, and I am the new President-Elect for the oldest and largest professional industry-driven cybersecurity information association in the world.

[Applause.]

Mr. MURRAY. Senator Hickenlooper, Chairman Cardin and other members of the Committee, thank you for this opportunity to address an area of national interest addressing cybersecurity concerns for small businesses in the United States. As a practitioner and educator, it is my intent to make you aware of some very important information which can be used to influence decisions related to information privacy and cybersecurity.

Today, we know that 80 percent of most organizations' business processes are automated, meaning that we are using some type of technology to process, transmit, or store information related to a job task that are performed by employees. There can be risk associated with these processes if the employees and business managers do not consider security as part of awareness. The following statistics associated with cybersecurity trends for small and mid-sized businesses include:

According to the National Cybersecurity Alliance, 70 percent of cyberattacks target small to mid-sized businesses. The Ponemon Institute reports that the average cost of a breach for small or mid-sized business, per incident, is \$383,000. According to the Better Business Bureau, 50 percent will become unprofitable within a month of being breached. Finally, Gartner published in its Top Trends in Cybersecurity 2023 report that 60 percent of small businesses that are victims of a cyberattack go out of business within 6 months, and overall, cybercrime costs small and medium businesses more than \$2.2 million a year.

In the 2023 Data Breach Investigations Report published by Verizon every year, "Ransomware continues to be a major threat for organizations of all sizes and industries and is present in 24 percent of breaches. Of those cases, 94 percent fall within system intrusion"; "74 percent of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials or social engineering"; "83 percent of breaches involved external actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95 percent."

The coronavirus pandemic saw a significant increase of remote workers and an investment of online technology, remote meeting applications, and cloud-based business resource subscriptions. The initial focus of small businesses was to get connected to resources. Unfortunately, security was often not considered until the business began experiencing data breaches, interception of remote meetings and unauthorized disclosure of sensitive information on non-company-owned devices. While cloud and remote computing have in-

creased productivity and business capabilities, they have increased the cyberattack terrain.

In the last 2 years our team at Murray Security Services performed assessments on small and medium-sized businesses in multiple industries and in multiple states across the country. Some of the top issues we have seen, personally, include social engineering people to disclose things like user names and passwords, sensitive product information and personal identifiable information; lack of dedicated IT or cybersecurity resources; uncontrolled access to sensitive areas of a building—if I can get physical access, the rest is even easier; sensitive information found in trash cans, dumpsters and in unattended workspaces; computer applications or equipment that are vulnerable to cyber-attacks due to missing patches or misconfigurations.

Cybersecurity is primarily about protecting information. Some of the most sensitive information that needs to be protected is privacy information. This means that the relationship between cybersecurity and privacy data and information is significant. While the United States has many various privacy laws related to highly regulated industries like banking and finance as well as healthcare, we do not yet have an overarching national privacy law such as the General Data Protection Regulation in the EU.

A current bill being considered, since 2019, called the “Safe Data Act” would address many of these areas. Instead, businesses have to navigate the complexity of 50 states’ privacy and cybersecurity laws, which can become overwhelming and very time consuming.

The United States provides, as Al mentioned, one of the largest procurements of small business resources. To be considered, businesses now have to comply with cybersecurity hygiene requirements as identified by FedRamp, the Cybersecurity Maturity Model Certification, as mentioned previously by Mr. Stine, the NIST Special Pub 800–171 Protecting Controlled Unclassified Information, CUL—another acronym—in nonfederal systems and organizations, as well as other requirements identified in the Federal Acquisition regulation.

Small businesses need access to free resources for education and training to understand these requirements. Based on recently passed legislation, SBDCs now require a cybersecurity lead center to support their small business clients to help address cyber issues. SBA should require additional dedicated funding to better develop standardized programs across SBDCs and SCOREs for consistent training and education as well as cyber-related resources to help protect small businesses. An example of this is the America’s SBDC North Star program which represents the overarching efforts of the America’s SBDC network to mitigate cyber threats to small businesses. Dedicated funding would allow consistent cyber programming instead of having to chase funding through grant proposals each year.

For small businesses, an additional resource to consider is the Center for Internet Security which provides CIS critical security controls and benchmarks for a prioritized set of actions to protect organizations and data from cyberattack vectors.

For small businesses the three primary areas to focus are security awareness and skills training, data recovery, and access con-

trol management. The National Institute of Standards and Technology provides additional guidance and resources as discussed in Mr. Stine's testimony.

In closing, cyber threats pose a significant challenge to our country, our businesses and to our national security. A disruption to commerce due to threat actors attacking businesses should be considered a serious threat to our economic viability. With the onset of new technological advances such as artificial intelligence and the Internet of Things, there needs to be dedicated resources to educate, train, and advise business owners and leaders on achieving appropriate cybersecurity hygiene to protect their business as well as their information.

Again, thank you for this opportunity to testify in front of you today.

[The prepared statement of Mr. Murray follows:]

Testimony of: Dr. Shawn P. Murray

President of Murray Security Services and  
President Elect of the Information Systems Security  
Association International Board of Directors

Before the United States Senate  
Committee on Small Business and Entrepreneurship

“Cybersecurity: Challenges and Opportunities for Small  
Businesses”

Field Hearing

August 15, 2023

Senator Hickenlooper, Chairman Cardin and other members of the Committee, thank you for this opportunity to address an area of national interest addressing cybersecurity concerns for small businesses in the United States. As a practitioner and educator, it is my intent to make you aware of some very important information which can be used to influence decisions related to information privacy and cybersecurity.

Today, we know that 80% of most organizations business processes are automated, meaning that we are using some type of technology to process, transmit or store information related to a job task that are performed by employees. There can be risk associated with these processes if the employees and business managers don't consider security as part of awareness. The following statistics associated with cybersecurity trends for small and mid-sized businesses include:

According to the National Cybersecurity Alliance, 70% of cyber-attacks target small to mid-sized businesses. The Ponemon Institute reports that the average cost of a breach for small and midsized businesses is 383k and according to the Better Business Bureau, 50% will become unprofitable within a month of being breached. Finally, Gartner published in its Top Trends in Cybersecurity 2023 report that 60% of small businesses that are victims of a cyber-attack go out of business within six months and overall, cybercrime costs small and medium businesses more than \$2.2 million a year.

In the 2023 Data Breach Investigations Report, Verizon reported that:

- “Ransomware continues to be a major threat for organizations of all sizes and industries and is present in 24% of breaches. Of those cases, 94% fall within System Intrusion.”
- “74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.”
- “83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.”

The Corona Virus Pandemic saw a significant increase of remote workers and an investment of online technology, remote meeting applications and cloud-based business resource subscriptions. The initial focus of small businesses was to get connected to resources. Unfortunately, security was often not considered until the business began experiencing data breaches, interception of remote meetings and unauthorized disclosure of sensitive information on non-company owned devices. While cloud and remote computing have increased productivity and business capabilities, they have increased the cyber attack terrain.

In the last two years our team performed assessments on small and medium sized businesses in multiple industries and in multiple states across the country. Some of the top issues we have seen include:

- Social engineering people to disclose things like user names and passwords, sensitive product information and personal identifiable information
- Lack of dedicated IT or cybersecurity resources
- Uncontrolled access to sensitive areas of a building.
- Sensitive information found in trash cans, dumpsters and in unattended workspaces.

- Computer applications or equipment that are vulnerable to cyber-attacks due to missing patches or misconfigurations.

Cybersecurity is primarily about protecting information. Some of the most sensitive information that needs to be protected is privacy information. This means that relationship between cybersecurity and privacy data and information is significant. While the United States has many various privacy laws related to highly regulated industries like banking & finance as well as healthcare, we do not yet have an overarching national privacy law such as the General Data Protection Regulation in the EU. A current bill being considered called the “Safe Data Act” would address many areas. Instead, businesses have to navigate the complexity of 50 states privacy and cybersecurity laws which can become overwhelming and time consuming.

The United States provides one of the largest procurements of small business resources. To be considered, businesses now have to comply with cybersecurity hygiene requirements as identified by FedRamp, the Cybersecurity Maturity Model Certification (CMMC), NIST SP 800-171 Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations as well as other requirements identified in the Federal Acquisition regulation.

Small businesses need access to free resources for education and training to understand these requirements.

Based on recently passed legislation, SBDCs now require a cybersecurity lead center to support their small business clients to help address cyber issues. SBA should require additional dedicated funding to better develop standardized programs across SBDCs and SCOREs for consistent Training & Education as well as cyber related resources to help protect small businesses. An example is the America’s SBDC North Star program which represents the overarching efforts of the America’s SBDC network to mitigate cyber threats to small businesses. Dedicated funding would allow consistent cyber programming instead of having to chase funding through grant proposals each year.

An additional resource to consider is the Center for Internet Security (CIS) which provides CIS Critical Security Controls and Benchmarks for prioritized set of actions to protect organizations and data from cyber-attack vectors.

For small businesses the three primary areas to focus are:

- Security Awareness and Skills Training, Data Recovery and Access Control Management

The National Institute of Standards and Technology provides additional guidance and resources as discussed in Mr. Stein’s testimony.

In closing, cyber threats pose a significant challenge to our country, our businesses and to our national security. A disruption to commerce due to threat actors attacking businesses should be considered a serious threat to our economic viability. With the onset of new technological advances such as Artificial Intelligence and the Internet of Things, there needs to be dedicated resources to educate, train and advise business owners and leaders on achieving appropriate cybersecurity hygiene to protect their business as well as their information.

Again, thank you for this opportunity to testify in front of this committee.

**Resources:**

Center for Internet Security (CIS) - <https://www.cisecurity.org/controls>

2023 Data Breach Investigations Report -  
<https://www.verizon.com/business/resources/reports/dbir/2023/small-business-data-breaches/>

Gartner Identifies the Top Cybersecurity Trends for 2023 -  
<https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023>

The Ponemon Institute - <https://www.ponemon.org>

Better Business Bureau - <https://www.bbb.org/>

North Star Program: Cybersecurity Guidance For Small Businesses -  
<https://americassbdc.org/cybersecurity/>

Senator HICKENLOOPER. Thank you, Shawn. I appreciate it. I appreciate all of you being here. I am so glad I gave you a chance to make your opening comments.

So I will repeat my first question that I so inelegantly began with. This is a bipartisan issue. It is going to require a whole-of-government response to make sure that we are able to allow small businesses to preempt the risk of cyberattacks. I appreciate Kevin's time with us today and all the work that NIST is doing, moved light years in a very short period of time.

Just each of you, just to start, what would be the one issue you would recommend we highlight as we work with the executive branch on the Federal Government on ways that small businesses can safeguard their data.

Ms. BLISS. Senator, because I am the educator on this panel, although you all are educators, we all do this, I think you need to make it a team sport, and we have to think about it longer term and look for very unique, diverse teams to solve not just the current problems but come up with a way, in that K-to-gray mindset, that we can then bring those students into this conversation so that we are not having people having the problems that we have today.

So if we have that baseline across the education system, then as people build their businesses they will build that resiliency in cybersecurity in because they will be aware of how to do that. Obviously, resource is a big part of that, and I know you guys will talk to that.

But I think the education and training piece of taking a non-traditional approach than we have had in the past with the silos, and this is how education works, or this is how training works, and blending that together, kind of like we are going to do on our grants—we are going to test it out—I think is the way we can move forward to solve the future problems. Because I feel like we are chasing our tails today, but if we look at it bigger term we can solve longer-term problems.

Senator HICKENLOOPER. Alfred.

Mr. ORTIZ. Senator, so my late father-in-law used to say education is the great equalizer, and I think the cyberspace is no different. I think if we can get these new businesses, these smaller businesses I mentioned before, and be able to educate those folks before they get an SBA loan, or before they take that next step, the same way that they would go get an attorney and an accountant to do their books, they should go take a couple of classes in cybersecurity at SBDC with one of us who is a certified-slash-educator in this space, and I think it would really help.

We are really on the next generation of where IT and cyber meets. You know, I am aging myself, but those Commodore 64's and all of those computers are old school, and we are now in that next generation or age. So I think education and certainly funding behind that to get these small businesses going will certainly take us to that next level.

Senator HICKENLOOPER. Great.

Mr. MURRAY. Senator, thanks. You know, my colleagues here have identified a lot of the training and education so I will take a different approach to it, and that is collaboration, collaboration, col-

laboration. Here in our own ecosystem there is so much that is going on here in our community, from IT and cyber perspective.

We looked at a capability to build a level of collaboration by creating a program called the Cyber Leadership Roundtable. Aikta Marcoulie, who is our Regional Director for SBA, was our SBDC Director at the time. She and I both co-chair that organization. We actually have a charter. We have various goals and objectives to be able to collaborate and achieve different things.

The idea here is we do not compete with cyber resources. So if our local chapter for ISSA is running an event, we will not run a different event to compete with it. We will collaborate with them, and we will share the space, and we will send out the message.

You know, the example of winning this grant is an example of that collaboration that came out of the Cyber Leadership Roundtable, where we now have multiple organizations that can collaborate together to get more opportunity to get grants and funding.

So state and local resource, look at your ecosystem, understand who the movers and shakers are, commit to be able to collaborate to solve problems.

Senator HICKENLOOPER. All right. Well, that collaboration, I could not agree more. More education, more collaboration, those are the two hallmarks. And in a funny way, when this facility was actually put together that idea of having education, universities collaborating with small businesses and larger businesses, but also working with government was kind of first and foremost in everybody's mind. And there is nothing stronger, and something that really does set us aside from most of our rivals in the world.

Gretchen, why don't I start with you in terms of the evolving state of the workforce in cybersecurity. As we move towards deploying more and more 5G networks and beyond and further enabling, let's call it, the Internet of Things everywhere, how is the demand for cybersecurity professionals going to change? How do you keep up with that?

Ms. BLISS. That is the million-dollar question.

Senator HICKENLOOPER. Who is going to pay me?

Ms. BLISS. You know, the issue with this is that when you think about education systems, a lot of times I use history as an example. My mom is a history professor. You know, the battles happened on a certain day and you get to learn that, and you get to put it in context. But in cybersecurity it changes every single day, and so that demand is that currency. We have to increase not only the numbers, we have to increase the diversity that we have in cybersecurity. We have to diversify the experience.

You know, as my example of all the programs across all the interdisciplinaries we have, plus the training and education piece that we do, I feel that we really have to be able to respond to the evolution of the threat, and that is something that we do chase our tails on. And if there is a way that we could tweak the education system so that it can be more dynamic and interactive, with industry, with government, again, that kind of team sport, if we can approach it that way, I think what is going to happen is that the professionals need to be that adaptable. They need to be able to move into different areas and not get stuck in stovepipes, which education tends to do.

But that hands-on experience piece that we get from our partners I think broadens that, so those students, those employees, that workforce can be a little more dynamic and respond in different industry sectors and create some sort of commonality between them.

Senator HICKENLOOPER. And in that evolving world of education, that assumes, I guess, a constantly changing and improving and more essential group of foundational concepts and applications that people have to learn, just to begin their journey.

Ms. BLISS. Absolutely. The thing I always say is it is a purple unicorn. You guys have heard me say this a lot. You have got to get a degree of some sort, you have got to get hands-on experience, and you have to get an industry credential, and educational programs do not necessarily wrap themselves around those three ideas.

So I feel like through the CAE program we are embracing that diversity to try and build programs that can be that dynamic and responsive.

Senator HICKENLOOPER. I agree. We sometimes lose track in the race for education that there is supposed to be a good job and a career attached to that.

Mr. Ortiz—I am going to call you Alfred, first thing. I have known Gretchen now. We are not a Washington—

Mr. ORTIZ. This is Colorado.

Senator HICKENLOOPER. Yeah, exactly. Alfred, we are going to take off our ties, you know.

Mr. ORTIZ. Where is that beer?

Senator HICKENLOOPER. Cyber insurance can help businesses respond to and recover from cyber incidents if they do occur. Our Insure Cybersecurity Act, which is a bill we worked on last year with Senator Capito from West Virginia, offers, or will someday offer clear information to businesses on how cyber insurance works and how it can make their business more cyber resilient.

How should small businesses evaluate cyber insurance, and is there some benefit to clear and simple information that helps them make better informed decisions?

Mr. ORTIZ. I think that it is a little bit tough in some instances with regard to the types of business you get into. So for example, if you have a small medical firm that is worried about HIPAA compliance and things of that nature the risk may be higher than if it were to be, let's say, automotive repair shop, like my father used to have. Where is that data? What type of risk is out there? And how much is that risk going to cost the owner of that company?

To the point that I think depending on the industry, whether it be NAIC codes that you could use to be able to say this particular code would say that this business has this level of risk, in general, may help with regard to appropriately getting the right amount of cyber insurance. So that could be a possible way to tie in the risk with the type of business vertical that you are looking at.

Obviously, the more, the better, but because of the amount of cyberattacks, that insurance amount may be going up as well.

Senator HICKENLOOPER. Yeah, and I think we talked about a little of this with Kevin, you know, having the right language so that

people understand these risks and maybe some of the increments as we become better able to understand them ourselves, would have value as well.

Mr. MURRAY. Senator, if I may add to that, the complexity of cyber insurance has grown significantly over just the last 5 years. It does not matter what size your business is. You know, initially when cyber insurance came out the underwriters were going like, "Cyber insurance? Free money," and then all of a sudden we started making claims and breaches, and the costs associated with those highly regulated industries, as Al mentioned.

Now, cybersecurity underwriters are putting in amount of rigor in your policy that says you will have antivirus, you will have an assessment, you will protect sensitive information or data, and if you do not, we are not going to pay the breach, to a point where you may have to have an assessment hired by the insurance company after a breach happens, and if they can prove that you did not do what you were supposed to, your due diligence, they are not going to pay anymore.

Senator HICKENLOOPER. All right. It is a little bit like the issues we face, different states face around insurance for wildfires. With climate change and deeper droughts all over the country we see greater risk, and the insurance companies are still trying to catch up. You cannot have wooden roofs. You cannot have scrub grass coming up to the side of your house, wooden decks, all those things that invite a fire. I think the same thing is true in cyber, right?

Mr. MURRAY. Right. It is evolving.

Senator HICKENLOOPER. Yeah. And the rate of change, and we were talking about this earlier when we were—our green room was not really green, but when we were talking beforehand—the rate of change is only accelerating, and I think that is going to really require the universities, the private sector, and government to really step and make sure that we can keep up so that small businesses do not get wiped away.

I thought some of the statistics, Shawn, that you gave of once you are breached what the possibility is that you end up out of business in a year was truly startling, and something certainly the SBA should be pushing out there.

Gretchen, small businesses—Shawn, you helped with the previous question so you almost lost your own question—small businesses owners are in industries often with comparatively less exposure to cyber threats. I am not aware of a brewpub that has been hacked yet. They are often focused on other priorities—building your sales, creating the team, running your business.

In your experience of cybersecurity training how aware would you say, on the broad arc of small business owners, how aware of they in various industries of digital threats and of the cost-effective strategies to be ready?

Mr. MURRAY. So it is a great question. I think all small businesses, whether it is Al's dad's automotive mechanic shop or it is the food truck or a hospitality organization, or a highly regulated industry, a small clinic, insurance company, my accountant, everyone is aware of the cyber threats these days. Certain world events like the invasion of Ukraine with Russia and all of a sudden there is a significance in how is Russia going to fund what it needs to

do. Well, ransomware, we still know, is one of the most significant areas where we have a lot of attacks, so we need to be aware of that. Small businesses were afraid of what was going to happen during that time frame.

So literally, a partnership with our SBDC, we came up with a white paper to pass out to all of our small business clients to educate them on what they could be doing and should be doing, and that is focusing on understanding what your critical assets are within your organization, understand what critical processes that you have. We had an electric company that they had one person that did payroll for a 54-person company. That person got in a car accident and was in a coma for 3 or 4 days. Nobody else knew how to do payroll.

So because that critical process was not understood, and they did not have that backup person, they hired us to come in, try and hack into the payroll system—well, you have an IT person, we can get it there, but where is it documented how they do payroll?

So luckily she came out in a few days and they were able to figure that out. In the meantime, we advised the client, go ahead and run the same payroll that you did, contact your bank, run the same payroll as you did last time. You will have to figure out who has got overtime, on vacation. But again, understanding the critical assets, those critical processes, understanding how to back those areas up.

And then the threat of that cyberattack, when we talk about the cyber threat itself, in educating, this is where the SBDCs come in. So that Cyber CYA program, Cover Your Assets, that program and its initial pilot allowed us to educate a select of about eight different businesses, where they got to participate in understanding their own business. We helped them identify their critical processes, their critical assets, and they had to develop a plan at the end. We actually did an assessment with them. At the end they had to come up with a plan.

And a partnership that we had with the Better Business Bureau stated if you actually execute your plan and you are a BBB member, we will give you a Cyber Badge of Honor on your BBB profile that says, “Hey, I am a business that is dedicated to protecting your information as well as mine.”

So those innovative programs to educate and train, outside of regular academia, I think are important.

Senator HICKENLOOPER. And so you guys chime in. Since we are not in Washington we can have a free-form discussion. Just do not tell anyone.

Where would people find out about these kinds of programs? Obviously you must have outreach through the SBA, SBDCs, and what have you, but also through your organization. How would the normal small business come across this if they were not connected to the SBA?

Mr. MURRAY. So it just comes about communities and resources. I think a lot of businesses during the pandemic came out because they were struggling. Where can I get resources, resources for training, you know, the Pikes Peak Workforce Center here in our community. I was advising my clients, there is all kinds of funding coming out of the current Administration providing upskilling for

just about any type of positions. But then I volunteered at my local Workforce Center board, and I learned so much about workforce and the things that help your community interact, and used those resources to educate the businesses that I was doing business with.

So one of the challenges—Tracy Marquez is the CEO of our Workforce Center. She is only allowed 10 percent for marketing for all of the programs that she puts out there. We have got to be able to release some of the restrictions on allowing us to educate the community about what resources are available.

The same restrictions apply to the SBDCs and some of the other programs. So the ability to allow us to market and get that word out would be a lot more advantageous.

Senator HICKENLOOPER. And again, when Kevin was talking about creating a language, that marketing, in a way, educates everybody and helps universalize that language.

Let me move on. Gretchen, small businesses, just the nature that they are small they already face stiff competition, whatever industry they are in, but this is especially true in those companies that do Federal contracting, and they are always against larger businesses. Usually the deck is stacked against them. The larger businesses have far more resources.

What can the SBA do to support small businesses so they have a strong cybersecurity posture and are positioned to secure contracts with the Federal Government?

Ms. BLISS. Well, I think a lot of it, I was particularly impressed with the way that the President's training and education strategy came out and talked about how you do not need to be alone and unafraid in this process. We need to build a coalition. We need to build those public-private partnerships. We need to build those conversations on education and training. And I feel like in an ecosystem where you have got all of those elements actively engaged you can create some wraparound and support for those small businesses to do those things. Because I believe the way the process is, too, between primes and subs, I think there is a really good conversation to have there where the primes can educate the subs and have it be part of their responsibility to protect—you go back to supply chain, you talked about supply chain.

And I also think the stuff that NIST is doing with the working group is a big part of getting that conversation and having them understand better the common vocabulary, the common language, and to create an understand. In education it is all about understanding, and I feel like all those efforts to educate in different ways, because not every student learns the same way, we create ten pathways for people to get to the same information just so they can get there and be able to use it in an active way to help support their company, to help be an active workforce member, or to help build the economy or a government entity.

So I feel like if we could do those things I think that is where the small businesses would then be able to compete on par with companies and partnered with companies to be able to win those government contracts.

Senator HICKENLOOPER. All right. And I think streamlining those requirements obviously is a big part of this in every way.

Alfred, NIST, SBA, all these agencies are working hard to try and help small businesses secure their data, but obviously the government cannot do this on its own. We have limited resources and the great American public wants to have this happen on a more universal scale.

How can we expand public-private partnerships in such a way that allows small businesses to get better cybersecurity protection?

Mr. ORTIZ. Well, I think there are a number of different ways, and something that Mr. Stine and I were talking about earlier was with respect to seeing how different states are handling it. If we look at some of the privacy requirements there is one for Colorado, there is one for California, Virginia, and other states. So if we were to move our business or to start up a business somewhere else, how would it be different with regard to some of those data requirements in different states? How do we make it so that it is somewhat universal, that there is some baseline, if you will, with regard to some of these frameworks that we are looking for, and in various areas?

So I think from a legislative standpoint, the European Union, for example, handles those GDPR privacy requirements, whereas in the United States we may enjoy our state independence from the Federal Government, but from a cyber perspective it may look a little bit different.

So looking at that, being able to get the word out. One of the things that I saw was something very important was last year, I believe it was March 22, where I was invited by the White House to speak at Denver Community College to entrepreneurs for the White House Economic Initiative. Some of those businesses that they saw did not realize PCR requirements with regard to payments, how important that data was. So we educated them a little bit on that. Their eyes did open quite big when they heard some of those.

And just the basics to be able to go out there and say, hey, this is the effort. It is affecting everybody, from the smallest player that maybe has a sub with a contract, we have already seen that it affects all of the bigger players as well, going back to Gretchen's point. And I will say it because it is a public case study, is the F-35 fighter jet. All the way from the bold step, the small tier three supply chain manufacturer got hacked because they did not have cybersecurity, went up to tier two, and then the main supplier. And now our adversaries have a copy of that in their back yard. So it affects everybody.

Senator HICKENLOOPER. Yeah, no, absolutely, and I think that vulnerability up and down the supply chain is something that people are just coming to grips with.

I hear all the time from small businesses that just of the simple protections, like dual authentication, you know, to make sure that people, when they sign on, log in, that they are taking some minimal, slightly inconvenient, but people are so used to their cellphones, their handheld devices, that they do not think they need that security, and obviously, you could not be further mistaken.

Shawn, many small businesses lack resources as the largest businesses to invest in these protections. Do you think there are incen-

tives that Congress should be considering, and what kind of incentives should we be considering to help small businesses make these early investments, within the recognition that obviously this has got to be something that is sustainable. In other words, this budget is going to be tighter than last year. I think next year's budget is going to be tighter than this year. We have to find ways of achieving this with minimal cost impact.

Mr. MURRAY. So great question. You know, we could go a thousand different directions on this, but I have got an example. Here is one that is near and dear, especially in this community, being a big government contractor, defense industrial base community. The CMMC is a great example, the Community Maturity Model Certification.

The initial release of CMMC was so rigorous and so significant that I heard complaints from small businesses that were already doing business with the government, stating, "Wow, I have got to invest in all of this cybersecurity and these programs, and I have got to get a certification, and I have got to understand all these controls, and I just build bolts that go on an aircraft that part of that supply chain, and there is risk associated with that. And now I have to do this to get the contract back again. So how do I justify the expense of all of this money, because all of the vendors, they jump onto whatever the latest and greatest technology is, they scare everybody, charge boatloads of money for it, and small businesses cannot sustain."

I helped two congressional members with an update to the National Defense Authorization Act, and we got an amendment passed that required a complete review of the CMMC, which then released CMMC 2.0, which addressed a lot of the small business concerns. There is now a platform that takes the NIST 800-171, Controlled Unclassified Information, and there are three tiers that focus just on one NIST artifact as opposed to ten different sources that are complex. There is a free website now where you can log into and start filling out everything that you need. There are videos educating you why you need to be doing what you are doing. And instead of five complex tiers you only have three now. And the program now is looked at so well that we are not looking at it just for DoD anymore. We are looking at it for the entire Federal Government, consistency.

So that is an example that I would suggest you take back to your team and consider other legislation that makes things like the SBDs, the SCOREs, or the other resources that are being funneled into programs that allow consistency across the Federal acquisition regulation, because the FAR is just so complex and it takes too long to get approved.

Senator HICKENLOOPER. All right. So the idea is that you would get through that initial investment and that would carry you everywhere.

Mr. MURRAY. Correct. Now you still have to do your due diligence and keep that up. But the initial expense up front, with no guarantee that you are going to get something in the end, that is where small businesses are concerned.

Senator HICKENLOOPER. Yeah, and I cannot blame them. No guarantee that they are going to get back that contract. There is

no guarantee that the investment will hold up. And from a number of people I have heard that they worry that they make those investments, and within 2 years there is a whole new set that they have got to come back with, and they have barely gotten their manufacturing line in place.

We are about out of time here. I am amazed I have not gotten the boot yet. But I am going to keep talking until they tell me to stop.

One of the things I was interested in, a couple of talked about whether there should be some sort of a boot camp for cybersecurity, that the Federal Government should help put together. How do you all think about that? I mean, it is obviously very difficult, for all the reasons you just described, to do something that was sufficiently meaningful to make it worth the investment of a small business owner's time and resources. But there is something also appealing about having something like that, that once you had created it, would allow people to feel confident that what they are investing in, it would have some sort of stamp of approval.

Mr. MURRAY. So I want to make sure I clarify before I respond. Are we talking about a boot camp for Congress? [Laughter.]

Senator HICKENLOOPER. There already is. It is called elections.

Mr. MURRAY. Right. Constituents and how we are getting that funding.

It is twofold. I would love to be able to share some of the stories that are absolutely real, and when you tell the story it really brings it home as to, wow, we have that same vulnerability, or we have that same issue, and that could be me, whereas, you know, going to academia and reading stuff, and this is an IP address, and this is how things communicate. But going out and understanding what that terrain looks like, and listening to other people's stories and how relevant it is, I think that is where it is going to bring it home. I think that is more meaningful—tell a story.

Mr. ORTIZ. I think from that standpoint there are a number of ways. I always look at maybe some of the smaller towns that have small businesses but do not have access to the NCCs of the world or UCCSs of the world and making it a point where even students could go, instead of taking a biology class they can say, "I can take a cyber class for my science class, and I can learn about this stuff and get exposed to it." So that is one way to be able to get it out to some of the smaller areas. And being able to have a road show, if you will, of these kinds of things, where small businesses can come into their local SBDC or Chamber of Commerce and listen to somebody talk, at least on those first things, as you mentioned, Senator, multifactor authentication, VPN, and the basics of passwords and so forth.

Senator HICKENLOOPER. All right. Gretchen.

Ms. BLISS. Yeah. The boot camp concept is very effective because it is time effective, it is depth and content effective, and it establishes that common understanding of vocabulary. And that goes back to Shawn's comments about consistency.

I did a research project once and looked at the 47 definitions that the government uses for cybersecurity. It is confusing. So if we can use something like that to create that common understanding and baseline I think it will help everyone to be successful and be able

to have that conversation. Because once you establish that baseline then you can respond in kind, into whatever industry, and things can be industry-unique.

We have constantly talked about having a level of certification, like a bar for a lawyer, right. Do we have something like that in cybersecurity? Are we getting there? What does that look like? You know, IEEE has the stuff that they do with their standards, and they have put cybersecurity in it as well.

So I feel like there are efforts out there, but they are not necessarily consolidated and consistent so that they can be accessible by everyone.

Senator HICKENLOOPER. That is a little bit like the Field of Dreams as well—if you build it, will they really come? I always worry that as effective as the Small Business Administration has been and the SBDCs, there are so many small businesses that are working so hard that they are not in the Chamber of Commerce. My small business, I never joined the Chamber of Commerce. I was in business for 15 years before I decided I was going to run for mayor of Denver.

But if you are really immersed in your small business, sometimes you are not in a place where you can see that, and I think a boot camp is the kind of thing that might actually bring people to the table that are not members anywhere, and I think that is a real issue.

Anyway, closing thoughts, any of you? I think we have probably taken a lot of your time, too much of your time.

Ms. BLISS. Not at all, sir. I just want to say thank you for your interest in this topic. As you know, cybersecurity is very broad, it is very deep, and sometimes we are all in a room talking about it and it is like touching the elephant. So I feel like efforts like this, and hearings like this help to broaden that context of conversation and understanding, and I appreciate you bringing it to Colorado Springs, because I feel like we have a very unique ecosystem here that we have been developing to have exactly the conversations that you are talking about. And we have kind of piloted some things, and we are going to keep doing that until we feel like we are getting it right.

So I really appreciate that, and just understand that the partnership here is going to continue to expand and build on the baseline that you have basically gotten in place with this effort over the last 10 years. So I really appreciate that.

Mr. ORTIZ. Senator, thank you for having us. I echo Gretchen's sentiments wholeheartedly. I think what we have got to do is collaborate with what Shawn was saying, come together, be able to put this first and foremost, as Americans, an all-partisan issue, as I had mentioned before, and put it out there so that we can all learn a little bit about cyber, so we can just keep our data safe, either as a business or personally, so we can be out there. And I think there are a number of folks that understand that, and we can all be neophytes to the message around cyber.

Mr. MURRAY. Thank you again, Senator and the Committee, for allowing us to come up and provide some testimony to be considered as you move back and make decisions. Remember that cybersecurity is about protecting information. It is a national security

issue, it is an economic issue, and both of them are tied together. We need to be able to protect the viability of our small businesses.

I cannot say any more. This has been a great venue. I appreciate you hosting us and allowing us to testify in front of you today.

Senator HICKENLOOPER. Thank you all, and I think a lot of the foundations that you led and that we heard from NIST and Kevin describing the importance of education and collaboration and creating this new language and getting the word out there. It does need to be just—several of you, or almost all of you, I think, at one time or another mentioned it, the analogy between accountants and your doctor or your attorney.

You know, I am from the school that actually believes you should not have to have your attorney on speed dial. I would like to get back to the time when you do not have so many rules and regulations. But I think within cybersecurity I think that is something that we are going to need. I probably just offended 200 lawyers. But the ability of our culture, our country, to really address this and make sure that everybody understands it somewhat in the way that everyone drives—if you go out on the roads, most people know “somewhat” how to drive a car. Sometimes we wonder.

But that awareness and that understanding of the basic principles has to expand. It has to get out there a lot faster. And you all being here and the work that you are doing every day is helping lead this country in that effort.

As a Senator I get to say on behalf of our country thank you for your help today and all your public service.

Now to conclude our hearing for today I would like to again, one last time, thank each of our witnesses for their testimony. I do hate calling you “witnesses” because it does imply a crime, which in this particular case I am not aware. There are many crimes around cybersecurity. I am not sure which one we are addressing.

We will keep the hearing record open for questions for 2 weeks, until August 28, 2023. We ask that witnesses submit their responses to those questions. As they come in we will get them to you and get us your responses by September 11, 2023.

With that this hearing is adjourned.

[Whereupon, at 4:02 p.m., the hearing was adjourned.]