AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 116–47

CYBER CRIME: AN EXISTENTIAL THREAT TO SMALL BUSINESS

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MARCH 13, 2019

Printed for the Committee on Small Business and Entrepreneurship

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

U.S. GOVERNMENT PUBLISHING OFFICE

36–838 PDF WASHINGTON : 2019

COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP

ONE HUNDRED SIXTEENTH CONGRESS

MARCO RUBIO, Florida, *Chairman*
BENJAMIN L. CARDIN, Maryland, *Ranking Member*

JAMES E. RISCH, Idaho
RAND PAUL, Kentucky
TIM SCOTT, South Carolina
JONI ERNST, Iowa
JAMES M. INHOFE, Oklahoma
TODD YOUNG, Indiana
JOHN KENNEDY, Louisiana
MITT ROMNEY, Utah
JOSH HAWLEY, Missouri

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

MICHAEL A. NEEDHAM, *Republican Staff Director*
SEAN MOORE, *Democratic Staff Director*

C O N T E N T S

Opening Statements

	Page
Rubio, Hon. Marco, Chairman, a U.S. Senator from Florida	1
Cardin, Hon. Benjamin L., Ranking Member, a U.S. Senator from Maryland	3

Witnesses

Panel 1

Roat, Ms. Maria, Chief Information Officer, U.S. Small Business Administration, Washington, DC	5
Romine, Dr. Charles, Director, Information Technology Laboratory, National Institute of Standards and Technology, Washington, DC	13

Panel 2

Smith, Ms. Stacey, President & CEO, Cyber Association of Maryland, Inc., Baltimore, MD	36
Hyman, Ms. Elizabeth, Executive Vice President, CompTIA, Washington, DC	41
Harper, Ms. Karen A., President, Charles River Analytics, Inc., Cambridge, MA	50

Alphabetical Listing

Cardin, Hon. Benjamin L.	
Opening statement	3
COLSA Corporation	
Statement dated March 26, 2019	92
Harper, Ms. Karen A.	
Testimony	50
Prepared statement	52
Responses to questions submitted by Chairman Rubio	89
Hyman, Ms. Elizabeth	
Testimony	41
Prepared statement	43
Responses to questions submitted by Chairman Rubio	86
Roat, Ms. Maria	
Testimony	5
Prepared statement	7
Responses to questions submitted by Chairman Rubio	72
Romine, Dr. Charles	
Testimony	13
Prepared statement	15
Responses to questions submitted by Chairman Rubio	78
Rubio, Hon. Marco	
Opening statement	1
Smith, Ms. Stacey	
Testimony	36
Prepared statement	39

CYBER CRIME: AN EXISTENTIAL THREAT TO SMALL BUSINESS

WEDNESDAY, MARCH 13, 2019

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

The Committee met, pursuant to notice, at 2:31 p.m., in Room 428A, Russell Senate Office Building, Hon. Marco Rubio, Chairman of the Committee, presiding.

Present: Senators Rubio, Scott, Ernst, Young, Kennedy, Hawley, Cardin, Cantwell, Shaheen, Markey, Duckworth, and Rosen.

OPENING STATEMENT OF HON. MARCO RUBIO, CHAIRMAN, A U.S. SENATOR FROM FLORIDA

Chairman RUBIO. The Senate Committee on Small Business and Entrepreneurship will come to order. I want to thank everyone that is here today, and I want to welcome our witnesses. We'll have two panels. I'll introduce them in a moment.

This hearing will discuss one of the most challenging issues facing small businesses: cybersecurity.

It's hard enough for small businesses to get up and running with changing markets, regulatory hurdles, and the cost of starting a business, but cyberattacks can bring a quick end to all of one's hard work.

Foreign hackers and other cyber criminals are increasingly targeting small businesses to steal their intellectual property, trade secrets, and valuable information, and an equally nefarious practice is to hold hostage small businesses' operational and customer data in order to get a ransom payment.

Small businesses are the victims in approximately 43 percent of all attacks. While ransomware attacks on individuals have fallen, those attacks, ransomware attacks targeting businesses, rose 12 percent in the last year. Almost 55 percent of small businesses were victim to phishing attacks in 2017. That is up 30 percent from just 2 years before that.

The risk of cybercrime is greater to small businesses, which lack, many cases, the dedicated IT staff, the sophisticated equipment that larger companies have in order to try and stay safe. Cybercriminals know that. They know small businesses may be unprepared for attacks, which is why small businesses are twice as likely to be targeted by phishing attacks.

Consequences of cybercrime are also greater for small businesses, which operate on a smaller profit margin and are not always able to bounce back after a costly attack.

The Department of Justice's Internet Crime Complaint Center recorded more than 300,000 cybersecurity complaints in 2017 alone, which added up to more than $1.4 billion in losses, and we know that cyberattacks on small businesses are significantly underreported because either they do not know who to call or they do not want their customers to know that they are, or have been, potentially compromised.

Because the risks to small businesses are so high today, I introduced, along with Senator Shaheen, the Small Business Cyber Training Act to create a cyber-strategy training program for the counselors at the small business development centers across the country. The bill will prepare them, these counselors, to provide vital advice on cybersecurity to entrepreneurs when it matters most: at the beginning of their businesses' life cycle. And perhaps, most importantly, counselors can make small businesses more aware of the very real cyber threats that they face.

In addition to internal controls and protections for their own operations, businesses that want to work with the Federal Government are required to meet an extra level of cybersecurity protection under NIST contracting requirements.

It is important for the Government to maintain a high level of security with its contractors, but the inability to meet certain cybersecurity criteria can begin to disqualify smaller companies, who cannot afford to build up the cyber capability necessary to service the Government.

In fact, many times small businesses cannot even understand what the Government requires of its contractors. It is complex. We hope that NIST, the SBA, and other Government agencies will work together to educate and train small business contractors so that they can be equipped to take on business with the Government.

Federal agencies face very real cyber threats, including the SBA. It may be a small Government agency in comparison to others, but for many small businesses, the SBA is an important gateway to loans, disaster relief, and business training. And that's why it's especially important that the IT system at the SBA be secure enough to protect very sensitive data that small businesses and lenders entrusted to the agency.

The SBA Office of Inspector General has consistently ranked SBA's IT as one of the most serious challenges facing the agency. Specifically, the IG has recommended that the SBA continue to improve IT controls to address operational risks, such as cyberattacks.

The SBA is moving quickly to modernize its systems, but we know that criminals often move even faster. In recent years, we have seen what happens when Government agencies let their guard down, as was the case with OPM in 2015 when personnel data of more than 4 million current and former Federal Government employees was stolen.

The risk of cyberattacks for small businesses also compromises data that could harm U.S. national security. Our adversaries are

laying the groundwork for cyber espionage by embedding their technology into the systems we depend on to do business, be it a small business or a Government business.

Just last week, reports emerged showing that the Chinese hacking group APT40 has infiltrated IT systems of at least 27 universities worldwide, including MIT, in an attempt to steal U.S. military information from less secure sources.

These cybercriminals operate with the full backing of the Chinese Communist Party, and we must take proactive steps to deny the Chinese government and others access to our networks and to the personal information of small businesses.

This is why I, along with the Rank Member Senator Cardin, introduced the SBA Cyber Awareness Act, which would require the SBA to develop a cyber strategy and to examine where the components in its IT system are manufactured.

This bill would also require the SBA to report to this Committee about the cyber breaches and threats it faces so that we can give the SBA the tools that it needs to defend itself against future attacks.

So we look forward to talking with our witnesses about ways to protect small business information from cybercriminals, while also helping them understand cyber guidelines and requirements that allow their full participation in the market.

Now I recognize the Ranking Member.

OPENING STATEMENT OF HON. BENJAMIN L. CARDIN, RANKING MEMBER, A U.S. SENATOR FROM MARYLAND

Senator CARDIN. Well, Mr. Chairman, first of all, thank you for convening this hearing on a very important topic for small businesses.

As I go around and meet with small business owners around the State of Maryland, around our Nation, cybersecurity and their capacity to deal with cyberattacks is always mentioned, and it is an area of great concern to the future growth of small businesses in our community.

In recent years, the Senate has played close attention to the risk that cybercrime poses to our national security and our democracy. We have also confronted the risk posed to consumers when their private data is exposed by hacks at large corporations and Federal agencies like Target, Equifax, and OPM.

As large companies and Government agencies continue to invest in cybersecurity and harden defenses, cybercriminals are increasingly turning their sights to softer targets, like small businesses that are unable to invest in the most cutting-edge cybersecurity technology.

According to the 2018 Verizon report, 58 percent of data breech victims globally are small businesses. Small businesses with their narrow margins and lower capital reserves are unable to maintain trained cybersecurity personnel or purchase the most up-to-date tools. So for most small businesses, a data breach is a fatal blow.

A 2017 Better Business Bureau survey revealed that more than half of all small businesses reported that they could not remain profitable for only—they could have remained profitable for only one month if they permanently lost access to the essential data,

and only 35 percent reported that they could survive more than 3 months. These statistics are cause of great concern.

So our goals for this hearing are twofold. First, we want to learn how SBA plans to comply with the Federal Data Management Standards outlined by the Federal IT Acquisition Reform Act, also known as FITARA. I was pleased to read last year's OIG report that found that the SBA has made substantial progress towards full compliance with FITARA. So I am looking forward to hearing from the SBA Chief Information Officer, Maria Roat, today about the tools and resources the SBA needs to achieve full compliance.

Second, we want to know how we can help small businesses keep their data out of the reach of cybercriminals. I am grateful to the National Institute of Standards and Technology, which is one of many Federal, commercial, and academic cybersecurity assets in my home State of Maryland. It is already working to improve cybersecurity for small businesses, and I am eager to examine what is working well but also interested in learning how NIST is tailoring its guidance into practical steps that small businesses can take.

Earlier this week, I was at NIST and had a chance to hear firsthand some of the work that you are doing. I am proud that in Maryland, we have the National Cybersecurity Center of Excellence, which partners with the State of Maryland, which provides incredible services in this challenging field.

We also have the Information Tech Lab at NIST, which is an important asset for us to have to try to understand how we can be more effective in dealing with this challenge.

Maryland is also home for U.S. Cyber Command, and we have University of Maryland. And, Mr. Chairman, I could go on and on about Maryland, but I know the State of Washington or Florida will want equal time. So I will move on.

Just that I am proud that Maryland is a national leader in helping to expand cybersecurity resources to small businesses so they can not only be prepared for cyber threats but recover when hackers strike.

Last year, our State enacted first-of-its-kind legislation to provide tax credits to small businesses that purchase cybersecurity products or services from a local qualified firm. The bill also created a tax credit for investors who invest in Maryland cybersecurity companies.

Stacey Smith, the executive director of Cyber Association of Maryland, is here to share some of the lessons we have learned in Maryland, so we have a better understanding of how to help small businesses with cybersecurity.

Lastly, I would like to thank all the witnesses that are here today that have joined us in this discussion. My hope is that by the end of this hearing, we will know where we are in our effort to keep the SBA and small businesses safe from cybercrime, a clear sense of where we need to go to ensure our data is kept safe, and ideas on the best way to achieve these results.

Thank you, Mr. Chairman.

Chairman RUBIO. Thank you.

And just claiming my time on behalf of Florida, we have no snow.

[Laughter.]

And I can see the Bahamas from my backyard.

All right. Our fist panel of witnesses is Ms. Maria Roat, the Chief Information Officer at the U.S. Small Business Administration. She previously served as the CIO at the Department of Transportation, was the Deputy CIO for FEMA, Chief of Staff and the CIO at DHS, and in numerous other Government IT roles. In addition, she retired from the U.S. Navy with the rank of Master Chief Petty Officer following 26 years of active duty and reserve service.

Charles Romine is the Director of the Information Technology Laboratory at the National Institute of Standards and Technology, NIST, under the Department of Commerce. At the ITL, Dr. Romine develops and disseminates the cybersecurity standards and guidelines for Federal agencies and U.S. industry. The ITL also uses emerging IT to help meet national priorities such as homeland security applications.

We all want to thank both of you for being here, and we will begin with you, Ms. Roat.

STATEMENT OF MARIA ROAT, CHIEF INFORMATION OFFICER, U.S. SMALL BUSINESS ADMINISTRATION, WASHINGTON, DC

Ms. ROAT. Thank you, Mr. Chairman, Ranking Member Cardin, and members of the Committee.

I joined SBA 2 and-a-half years ago after serving as the Chief Technology Officer at the Department of Transportation. Prior to that, I worked for 10 years at the Department of Homeland Security. At the time I came on board at SBA, the agency had experienced eight CIOs over a 10-year period. The lack of consistency negatively impacted the agency's technology footprint, and since taking over the position, my team and I have tackled many issues head on.

I am pleased to present a different picture today than what I inherited. We significantly upgraded the agency's technology stack and through comprehensive improvements generated $11 million in savings and cost avoidance.

Along the way, I have enjoyed the support of Administrator McMahon. I am proud of the work of my team and colleagues.

Under my direction, we continue to drive innovation and move aggressively to address deficiencies and improve SBA's cybersecurity posture. The result is that SBA is now a leading Federal agency in its cybersecurity capabilities.

Today, SBA employees have greater access to secure modern technology and productivity tools. Small businesses and entrepreneurs have an improved user experience, and they can be assured that we are protecting their information assets.

A key part of achieving this is taking an enterprise approach to modernization and moving our application systems and data to the cloud. In early 2017, we were the first agency to deploy DHS's Continuous Diagnostics and Mitigation, CDM, into the cloud. We ingest data from our on-prem assets, multiple cloud services, and even legacy IT to provide a detailed picture of our environment. This greatly reduced the number of tools and services in use while strengthening protection and detection capabilities.

Like many organizations, the number one threat to SBA is email. Phishing attacks are not just a nuisance. They are a serious and effective means to gain unauthorized access to sensitive information.

Over the past 6 months, my cybersecurity team identified and investigated nearly 500 phishing attacks. We purged over 6,800 malicious emails from employee mailboxes, and working with DHS, we removed nearly 300 malicious internet websites that were being used for phishing or distribution of malware.

The agency's website at sba.gov is the first place many small business owners engage with SBA, and the site receives more than 10 million unique visitors per year.

In 2018, during National Small Business Week, we launched our agency website to simplify customer access to SBA services.

In addition to this complete website re-platforming and design, my office continues to partner with our program offices to introduce modern technologies, help them manage large datasets, and develop much needed system improvements for our small business community.

In 2017, we worked with the Office of Capital Access to launch the Lender Match Tool to better connect borrowers with lenders. We helped the Office of Disaster Assistance deploy a new disaster credit management system to enhance our disaster loan processing. We are working with our Office of Investment and Innovation on a new platform for our SBIC program to allow us to better manage the lifecycle of SBICs.

We are beginning a project with our Office of Capital Access to replace our micro loan IT system to better manage data and loan information.

We will soon engage our Office of Entrepreneurial Development to replace the centralized Web-based reporting system used by our resource partners: SBDCs, SCOREs, Women Business Centers, and our Veteran Business Outreach Centers.

And we continue to support the work of Administrator McMahon on the launch of the new Women's Digital Learning Platform. I believe she discussed this with you during a recent testimony before the Committee.

These are examples of actions that are helping transform SBA from an agency with many stovepipes, unstable technology and infrastructure, to a more proactive and innovative enterprise services organization. We are becoming much more responsive to the business technology needs of SBA program offices, and we are recognized across the Federal and industry IT community as a technology leader and innovator. We have certainly come a long way in a short period of time.

Thank you for the opportunity to speak with you today. I look forward to your questions.

[The prepared statement of Ms. Roat follows:]

Statement of Maria Roat
Chief Information Officer
U.S. Small Business Administration

before the
Senate Committee on Small Business and Entrepreneurship

Hearing on "Cyber Crime: An Existential Threat to Small Business"
March 13, 2019

Statement of Maria Roat
Chief Information Officer
U.S. Small Business Administration

Chairman Rubio, Ranking Member Cardin, and members of the committee, thank you for the opportunity to discuss how the Small Business Administration (SBA) has transformed information technology and cybersecurity to protect business and protect entrepreneur's information assets.

In congressional testimony before the House Small Business Committee in July of 2017, I discussed information technology (IT) challenges at SBA and shared with members a history of the position at the agency. Prior to my arrival, the agency had eight different Chief Information Officers (CIO) over a ten year period. The lack of consistency in the position severely limited the agency, and since taking over the position, my team and I have addressed and tackled many issues head on. I am proud to present a different picture of the agency today. Along the way, I have enjoyed the support and leadership of Administrator Linda McMahon and I appreciate the hard work of our team and my colleagues at SBA.

Under my direction, the Office of the Chief Information Officer (OCIO) continues to move aggressively to address security deficiencies and to improve SBA's cybersecurity posture, governance and oversight, stabilize and modernize SBA's networks, systems, data centers, and overall operations. SBA's digital transformation benefits are two-fold. First, SBA employees have greater access to secure, modern technology and productivity tools. Second, small businesses and entrepreneur's user experience is enhanced. While we are driving innovation and rapid transformation, we are approaching security by design by building it in, not bolting it on. Cybersecurity improvements are frequently accomplished behind the scenes, integrated into solutions from the ground up, and are integral to protecting SBA's data. SBA is a leading federal agency in its cybersecurity capabilities, and I continue to be relentless in driving innovation to secure SBA's information assets.

Enterprise Cybersecurity Strategy

When it comes to protecting the small businesses and entrepreneurs we serve, it starts with protecting the valuable information entrusted to us. SBA hired a Chief Information Security Officer to design, build and lead a next generation cybersecurity program. I evaluated how and where the agency was spending its cybersecurity funds, and a year ago refocused and increased the cybersecurity spend. Last summer, my office produced the agency's first cybersecurity and privacy strategy to set the direction of cybersecurity for the agency. The strategy includes key cybersecurity and privacy principles with an emphasis on innovation and resilience. These requisite actions were taken to promote the cybersecurity transformation that I will now describe.

Strategies to Secure SBA's Digital Assets

As SBA moves its systems and data to the cloud, it is imperative that I create a comprehensive and central view of the SBA enterprise that includes multiple cloud; cloud-based services; our district and field offices, headquarters, and a mobile workforce. Integration in a meaningful way enables robust protection and detection of anomalies and is a challenge in any organization on a modernization and transformation journey. As my team and I grappled with

how to establish a fundamental architecture that considered all cloud and traditional requirements and addressed cybersecurity challenges, we had a realization. The vantage point offered from the cloud greatly simplified many of the challenges we were facing. This simple change in perspective, from a traditional on-premise model, to a cloud centered architecture, allowed us to establish an agency-wide view of all IT systems, services and all network traffic without having to add and maintain hardware and software. Taking a cloud-centric approach significantly reduced the number of tools and services in use while greatly strengthening and extending protection and detection capabilities by leveraging native cloud Artificial Intelligence and machine learning.

Under my direction, we modernized and consolidated cybersecurity management and introduced several capabilities that were limited or missing from the program. First, I now provide 24/7/365 security monitoring and incident response instead of providing these services just during the work week, as had been performed previously. Second, I created dedicated teams to perform continuous penetration testing, forensics analysis, and cyber threat hunting. I also expanded employee awareness through phishing exercises and cyber alerts. Third, we held 13 tabletop exercises with program office IT personnel simulating real-world scenarios to help them understand how to deal with cyberattacks. All these activities incorporate information from my cyber threat intelligence team that keeps track of threat actors likely to target financial or government sector organizations. The Chief Information Security Officer provides me daily incident reports and threat assessments.

Last fall, I officially launched five enterprise cybersecurity services at SBA to centralize visibility across program office IT and establish uniform incident response processes that protect the data that SBA maintains and manages for its services to small businesses and entrepreneurs. The five services are 24/7 security monitoring, incident response, vulnerability management, patch management, and continuous penetration testing. These services are critical components to any cyber program and add tremendous value protecting SBA and the small business community. SBA has also achieved cost savings by eliminating duplicative tools and management overhead.

The agency previously struggled with establishing and maintaining fundamental IT services, as noted in several OIG and GAO reports containing longstanding findings. When I arrived in October 2016, the agency had about 50 open OIG recommendations addressed to the CIO, many longstanding and delayed. I value the role of our auditors and strive to make their jobs a bit harder by establishing well managed programs and services. I'm happy to report that I established rigorous management of all audit findings and that the current number of open OIG recommendations now stands at 8. These 8 remaining findings are the most complex issues involving legacy and sometimes critical systems that we are working to modernize over the next 2 years.

Last year, I launched an Enterprise Customer Relationship Management (CRM) project. The goal of this initiative is to simplify access to SBA services for our customers. Establishing a single, complete view of each customer not only reduces errors and minimizes overhead, it also eliminates duplicative sensitive information which reduces the cost and complexity of security.

Like many organizations, the number one threat vector to SBA is email. Phishing attacks are not just a nuisance, they are a serious and very effective means to gain unauthorized access and exfiltrate sensitive information. My cybersecurity team places a heavy focus on phishing, from the monthly phishing exercises that we send to all SBA employees, to the continuous monitoring of agency email. Over the past 6 months, my team identified and investigated nearly 500 phishing attacks. They've purged over 6800 malicious emails from employee's mailboxes, often before the employee arrives at work. The SBA cybersecurity team identified and then worked with the Department of Homeland Security (DHS) to remove nearly 300 malicious Internet web sites that were being used for phishing or distribution of malware. Taking these sites down not only protects SBA, it also helps any other person, business or agency targeted by the same attack.

SBA.gov is the first place many small business owners engage with SBA for small business federal assistance when "googling" on the web. The SBA.gov digital product roughly receives around 10+ million unique visitors per year, making it unquestionably a much-needed resource to assist entrepreneurs and enable transparency for the agency. Over the last year we worked to continue modernization around the platform, including moving it to the cloud, unleashing a more reliable, secure platform. SBA's website now runs on immutable infrastructure that dynamically scales up to meet increasing traffic demands and elastically scales down when traffic reduces during off periods, such as nights and weekends. If an individual server is attacked or taken offline, then that server is replaced within 90 seconds by the system itself. This has tremendous benefits for the agency's digital presence in terms of its reliability and security, and ensuring the content presented to the small business is not "spoofed". The agency also saves on costs as well because the system is elastic, meaning parts of the system shut off when they are not needed.

Last year, the SBA began the configuration of an off-the-shelf cloud-based Software as a Service (SaaS) to provide fully modernized oversight and risk management tools for SBA's Office of Investment and Innovation (OII) to utilize in connection with all aspects of the Small Business Investment Company (SBIC) program. The single platform will be used to manage the entire life cycle of an SBIC--from the initial inquiry for fund managers interested in applying, the licensing application and approval process, operations oversight during the 10+ year period of an SBIC's lifecycle, coordination of regulatory examinations, and finally, the wind-up or liquidation of SBICs. The off-the-shelf solution will be deployed in SBA's cloud environment. By deploying the solution in SBA's cloud, it ensured that the solution complies with the Federal Risk and Management Program requirement. Further, data integrity and information asset protections are increased through the consolidation of over 105 gigabytes of data in 1,590 database tables from different workflows into a single structured data warehouse.

This year, SBA began working on the development of a Single Sign On portal designed to manage user authorizations (access) to SBA application services. The system will federate user identities from various authentication systems and provide role-based access control to downstream applications. This will significantly improve security by reducing the number of existing systems used to authorize user access to SBA resources. Additionally, it will enable a standard workflow for tracking authorizations and enable the application of uniform security policies.

Influencing Government Cybersecurity Strategies

Because of our significant progress in cybersecurity, SBA was selected by the Office of Management and Budget (OMB) to conduct a pilot to update the federal Trusted Internet Connection (TIC) policy. Through our cloud modernization achievements, we were able to demonstrate how native cloud tools, services and capabilities could meet and exceed objectives identified in the current TIC architecture. Our findings informed recent updates to the federal TIC policy, and SBA also demonstrated these capabilities to over 30 federal agencies and 300 attendees.

In 2017, SBA was the first federal agency to implement the DHS Continuous Diagnostics and Mitigation Program (CDM) in the cloud instead of a traditional on-premise implementation. SBA avoided a significant capital investment in hardware and accelerated the implementation. At the request of the Federal Deputy CIO, SBA recently proposed a proof of concept to expand on the success of the TIC modernization pilot to replace the traditional CDM capabilities with cloud-based tools similar to those utilized in the TIC pilot. Offering alternatives to achieving fundamental cyber hygiene capabilities will allow agencies flexibility when negotiating trade-offs between cost, security and functionality

Risk Management over Information Assets

Effective risk management practices are integral to protecting SBA's information assets. It is critical that I ensure SBA's IT, cybersecurity and privacy policies and practices align and support federal, regulatory and legislative requirements and protects SBA's information assets. I apply IT governance approaches to bring together IT, mission/business, procurement, finance, human resources, privacy, cybersecurity, and risk management to be the right authority with the right information, at the right time to make the best possible decisions to effectively deliver secure IT programs. Through a stronger governance model, I have greater visibility to improve cybersecurity planning, identify cost savings opportunities and to better understand and direct current and planned cyber security resources. The Chief Information Security Officer ensures that variances that result in risk exposures are made known at the leadership level to inform decisions on risk acceptance and/or mitigation, or resources to address the risk.

Assisting our Nation's Small Businesses with Cybersecurity

In addition to the steps we've taken to secure our agency operations, SBA also helps identify resources available to America's small businesses, including DHS's Cybersecurity and Infrastructure Security Agency (CISA). CISA is the primary interface for enterprises of all sizes to receive and share cyber threat indicators and defensive measures with the federal government. Since passage of the Cybersecurity Act of 2015, the federal government provides liability protections in limited circumstances to incentivize sharing this type of information with CISA. CISA also provides small businesses with a full range of technical assistance to include cybersecurity vulnerability assessment and incident response, as well as guidance on cybersecurity best practices.

Conclusion

Actions taken over the last two and a half years have transformed SBA from an agency with unstable technology and infrastructure, stovepipes, duplication and significant gaps, no cybersecurity strategy or operational control to a more proactive and innovative enterprise

services organization. We are now much more responsive to the business technology needs of SBA program offices and have been recognized by the Federal Chief Information Officer and across the federal and industry IT community as a technology leader and innovator. OCIO's partnership with SBA's program offices to introduce modern technologies, develop technology roadmaps, develop and migrate key applications to the cloud and develop approaches to ingest, store and manage large data sets is resulting in significant improvements to protect SBA's data and the small business community.

Chairman RUBIO. Thank you.
Dr. Romine.

STATEMENT OF CHARLES ROMINE, Ph.D., DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Dr. ROMINE. Chairman Rubio, Ranking Member Cardin, and members of the Committee, thank you for the opportunity to appear before you today to discuss NIST's cybersecurity efforts as they relate to small businesses.

Small businesses are more innovative, agile, and productive than ever, thanks to the capabilities delivered by information technology, but the IT security challenge for small businesses looms larger than ever.

In the cybersecurity realm, NIST has worked with Federal agencies, industry, and academia since 1972, and NIST's role has been expanded to research, develop, and deploy information security standards and technology to protect the Federal Government's information systems against threats as well as to facilitate and support the development of voluntary industry-led cybersecurity standards and best practices for critical information.

NIST has a longstanding and ongoing effort supporting small business cybersecurity. This is accomplished by providing guidance through publications, meetings, and events.

NIST has worked with interagency partners, including the Small Business Administration, the Federal Trade Commission, Federal Bureau of Investigations' InfraGard program, and DHS's Cybersecurity and Infrastructure Security Agency to host cybersecurity workshops, training webinars, and has provided online resources for small businesses.

More recently, in response to the NIST Small Business Cybersecurity Act, NIST launched the NIST Small Business Cybersecurity Corner website to put key resources in one place. Small Business Administration, CISA within the Department of Homeland Security, and Federal Trade Commission are contributors to this website. These agencies as well as nonprofit organizations are providing small business-focused resources to be shared through that site, and they will promote awareness and use of the site.

In 2016, NIST released a major revision to the popular report "Small Business Information Security: The Fundamentals." The report is designed for small business owners with little cybersecurity expertise and provides basic steps needed to help protect their information systems.

I would like to highlight a document that the Committee may be familiar with, "The Framework for Improving Critical Infrastructure Cybersecurity," or the Cybersecurity Framework, which many organizations, including many small businesses, use to manage their cybersecurity risk.

Published in 2014 and revised in 2017 and 2018, the framework provides a voluntary, risk-based, flexible, repeatable, and cost-effective approach that relies on voluntary standards, guidelines, and practices to help organizations identify, assess, manage, and communicate cybersecurity risks.

In addition to the Cybersecurity Framework, NIST has developed extensive cybersecurity standards and guidelines, including a risk management framework that can be customized for small businesses and implemented on a voluntary basis to help protect a small business' intellectual property and organizational assets.

Building further on the success of the Cybersecurity Framework, NIST released the draft Baldrige Cybersecurity Excellence Builder, a self-assessment tool to help organizations of all sizes better understand the effectiveness of their cybersecurity risk management efforts.

Small businesses constitute the backbone of the U.S. manufacturing sector. Within NIST, the Manufacturing Extension Partnership, or MEP, has a specific focus on assistance to small manufacturers and operates a nationwide network with MEP centers located in every U.S. State and Puerto Rico.

In 2008, the National Initiative for Cybersecurity Education, or NICE, a public-private collaboration among Government, academic, and industry, was established to enhance the overall cybersecurity capabilities of the United States.

In August 2017, NIST released the NICE framework, which is a national resource that categorizes and describes cybersecurity work.

The NIST National Cybersecurity Center of Excellence is a collaborative hub where industry organizations, Government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practice cybersecurity solutions for specific industries as well as for broad cross-sector technology challenges.

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

Thank you for the opportunity to present NIST views regarding cybersecurity challenges facing small businesses, and I will be pleased to answer any questions that you may have.

[The prepared statement of Dr. Romine follows:]

Testimony of

Charles H. Romine, Ph.D.

Director

Information Technology Laboratory

National Institute of Standards and Technology

United States Department of Commerce

Before the

United States Senate

Committee on Small Business and Entrepreneurship

"Cyber Crime: An Existential Threat to Small Business"

March 13, 2019

Introduction

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

NIST Role in Cybersecurity

Home to five Nobel Prizes, with programs focused on national priorities such as advanced manufacturing, the digital economy, precision metrology, quantum science, and biosciences, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, when it helped develop and published the data encryption standard, which enabled efficiencies like electronic banking that we all enjoy today. NIST's role, to research, develop, and deploy information security standards and technology to protect the Federal Government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347)[1] and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies as well as businesses of all sizes, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, state-of-art and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

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

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

Small Business Role

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

Cybersecurity is vitally important to a business' bottom line. Cybersecurity breaches cost businesses billions of dollars in lost revenue and loss of productivity every year. The impact on reputation and the loss of customers' trust can cause long-term damage to a small business. A vulnerability common to a large percentage of small businesses could pose a significant threat to the Nation's economy and overall security. Many of these businesses house sensitive personal information including healthcare or financial information. Many small businesses also provide services to the federal, state, local and tribal governments and have access to government information or systems. In the interconnected environment in which Americans currently operate, it is vital that small businesses are aware of and actively manage cyber risks.

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

When implementing new technologies, small businesses need to fully understand all of the potential security risks created by connecting to the Internet. The risks to systems are so complex and pervasive that one cannot reasonably expect small businesses to be experts in all areas of security, including properly implementing security controls for complex system configurations and assessing security features associated with new and emerging technology.

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

---

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

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

NIST Small Business Cybersecurity Corner

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

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

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

Cybersecurity Framework

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

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

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

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

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

Cybersecurity Fundamentals

In November 2016, NIST released a major revision to the popular report Small Business Information Security: The Fundamentals[9] (NIST Interagency Report, NISTIR 7621R1). The report is designed for small business owners with little cybersecurity expertise and provides basic steps needed to help protect their information systems. NISTIR 7621R1 guides readers through a simple risk assessment to understand the organization's vulnerabilities. After identifying and determining the value of the organization's information, the users evaluate the risk to the business and customers if its confidentiality, integrity, or availability were compromised.

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

Risk Management Framework

In addition to the Cybersecurity Framework, NIST has developed, over the past decade, an extensive set of cybersecurity standards and guidelines, including a Risk Management Framework (RMF), that can be customized for small businesses and implemented on a voluntary basis to help protect a small business's intellectual property and organizational assets. The flexibility of the RMF is backed up by a set of comprehensive, state-of-the-practice security and privacy controls that can help small businesses be less susceptible to a range of cyber threats that can impact their competitiveness and survivability in a high risk, Internet-based operating environment. NIST released the second version of Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations*,[10] in December 2018, after receiving

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

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

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

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

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

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

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

Cybersecurity for Small U.S. Manufacturers

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

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

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

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

Baldrige-Based Tool for Cybersecurity Excellence

Building further on the success of the Cybersecurity Framework, NIST released the draft Baldrige Cybersecurity Excellence Builder,[13] a self-assessment tool to help organizations of all sizes better understand the effectiveness of their cybersecurity risk management efforts. The Builder blends the best of two globally recognized and widely used NIST resources: the organizational performance evaluation strategies from the Baldrige Performance Excellence Program and the risk management mechanisms of the Cybersecurity Framework. Using the Builder, organizations of all sizes and types can:

- Determine cybersecurity-related activities that are important to business strategy and the delivery of critical services;
- Prioritize investments in managing cybersecurity risk;
- Assess the effectiveness and efficiency in using cybersecurity standards, guidelines, and practices;
- Assess their cybersecurity results; and
- Identify priorities for improvement.

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

National Initiative for Cybersecurity Education

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

In 2008, the National Initiative for Cybersecurity Education (NICE), a public-private collaboration among government, academia, and industry, was established to enhance the overall cybersecurity capabilities of the United States. The NICE program seeks to energize and

[12] https://www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security

[13] https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative#bceb

promote a robust ecosystem for cybersecurity education, training, and workforce development. As the lead agency for this initiative, NIST works with more than 20 federal departments and agencies, as well as with industry and academia, to ensure a digital economy enabled by a knowledgeable and skilled cybersecurity workforce.

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

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

National Cybersecurity Center of Excellence

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

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

---

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

Conclusion

Small businesses are more innovative, agile, and productive than ever, thanks to the capabilities delivered by information technology, but the IT security challenge for small businesses looms larger than ever. Systems managed by small businesses are part of a large, interconnected community enabled by extensive networks and increased computing power. Small businesses must take steps to secure systems against malicious activity, or accidental unauthorized disclosure of sensitive information or breach of privacy.

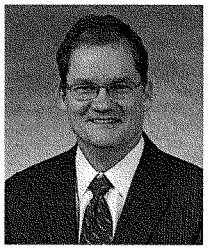
NIST recognizes that it has an essential role to play in helping small businesses. The NIST programs described here demonstrate that NIST's cybersecurity portfolio is applicable to a wide variety of users, from small and medium-sized enterprises to large private and public organizations.

NIST is fiercely proud of its role in establishing and improving the comprehensive set of cybersecurity technical solutions, standards, guidelines, and best practices, and of the robust collaborations enjoyed with its Federal government partners, private sector collaborators, and international colleagues.

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

24

Charles H. Romine



Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of seven research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of $160 million, nearly 400 employees, and approximately 300 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission, to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the Nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

Education:

Ph.D. in Applied Mathematics from the University of Virginia.

B.A. in Mathematics from the University of Virginia.

Chairman RUBIO. Thank you both.

I am going to defer the majority of my time at the front end.

I just want to start actually with a story and then a kind of comment. I would love your input on this.

So, about 2 years ago, according to an account that was shared with me, a small midsized company in South Florida shared with me that they got to work on a Monday morning and found that their entire system had been locked, and they had gotten, somehow, notification. I believe they said by email, but basically, all of their financial and proprietary business records had been stolen. And that in the message, they basically said to them, "We want you to send us $500,000 in Bitcoin. We know you can afford it because we have your financials. We are not asking for a million. We are asking $500,000."

They contacted law enforcement and were basically told, well, if you want your information back, you are going to have to pay it.

This was a company that—I would not say they are tiny. They are certainly profitable and a growing business but certainly not a large company. They had bars on the windows and an alarm system in their office, but they were wholly unaware that anybody even knew they existed, much less that a foreign actor from North Korea or somewhere else would target them.

What do you assess writ large is the awareness that exists today among the millions of small and midsized businesses in America that they can be targeted this way, and what are we doing to create more awareness that this could happen to them?

Dr. ROMINE. Well, thank you, Mr. Chairman, for the question.

It is certainly the case that businesses of all sizes are susceptible to cybersecurity risk, and I think we are seeing increasingly that that is manifested through attacks on organizations of all sizes, so I understand the concern.

From our perspective, from the NIST perspective, the way that we manage that is by trying to communicate more effectively to small and medium businesses that the size of your organization does not make you immune to the potential for cyber risk and that you have a responsibility in the same way that every organization manages financial risk and reputational risk and HR risk and all other types of risk. You have a responsibility as an organization to also manage your cybersecurity risk.

Now, stating that after the fact, after someone has been attacked, I am not trying to blame the victim here. I am just saying that the goal for NIST is to try to raise that awareness across all sectors of the economy and at all scales that there is a responsibility to manage that risk, and that we have resources available that can help you do that.

Chairman RUBIO. What's your sense of the general awareness? I know it is not directly your department but just interacting with this issue.

Ms. ROAT. So with the SBA, I think the Small Business Development Center is working with the Office of Entrepreneurial Development. Working with those small businesses, many times it is not that the tools are not there and toolkits are not there, but I think there needs to be more engagement and more communication with

the small businesses to get out in front of that and facilitation and getting that information sharing out there.

You can tell a small business, "Protect your enforcement," but how do you do it? What is that checklist? I think there needs to be more engagement on that, adding on to what Dr. Romine said.

Chairman RUBIO. Ranking Member.

Senator CARDIN. Well, thank both of you for your testimony.

Ms. Roat, on April 25th of last year, this Committee held a hearing in regards to preparing small businesses for cybersecurity success. After that hearing, then Chairman Risch and I sent a letter to Administrator McMahon with some of the suggestions that came out of that hearing, and we asked her view on requiring a number of Small Business Development Center counselors to be certified in cybersecurity assistance, a certification program for part-time cybersecurity professionals to fill the void that exists and IT workers that will service small businesses, a cybersecurity boot camp for small businesses, and forming a cybersecurity co-op to pull together willing buyers from various cybersecurity products and services, lowering the costs to small businesses for these products.

We have not gotten a reply to that letter. Are you aware that that letter was sent, and can you just tell us what progress has been made in regards to those suggestions?

Ms. ROAT. So I am aware of the letter. I think in the context of the work that SBA's Office of Entrepreneurial Development has done with DHS, they are working on the Small Business Development Center, the cyber strategy for those small businesses, those SBDCs, and I think some of the elements that are in that letter should be incorporated as part of what should be done as part of that plan.

I know that plan is in final clearance right now, but those elements should be at least vetted and worked through as part of that plan with SBA, the Office of Entrepreneurial Development, the SBDCs, as well as DHS.

Senator CARDIN. So when can we expect to receive that?

Ms. ROAT. It is in final clearance right now, going through SBA and DHS.

Senator CARDIN. A couple weeks? A month?

Ms. ROAT. I am not entirely sure. I do know that it is complete, and it is being vetted through SBA up to the Administrator now and through DHS.

Senator CARDIN. Well, I would encourage you to try to get that to us, particularly in response to our letter.

There was an OIG report dealing with SBA's most serious management and performance challenges, and several categories, the OIG report gives you progress for implementing the recommendations. However, the OIG report also states at SBA, outstanding IT security vulnerabilities remain, and the agency had significant deficiencies in IT security controls.

Can you tell us the progress in implementing those recommendations or those findings?

Ms. ROAT. So the original management challenges, they were handed to me in October of 2016 when I walked in the door at SBA.

I can tell you over the last 2 years, we have made significant progress, and we have actually taken not small steps, but very big steps to improve our cybersecurity posture at SBA.

Not only have we gotten our arms around the entire technology stack from the infrastructure upgrading, all of our servers patching, we have consolidated our tool sets. We are now using cloud-based tool sets to monitoring all of our on-prem environment, all of our cloud-based environments. We are taking log data, and that includes our legacy systems, taking all that data. So we have visibility of our entire enterprise.

We are current on our patch levels across the entire organization. We are not running old operating systems and anything like that anymore. We have taken care of that. We have gotten rid of old equipment, old hardware, old software, and we have consolidated a lot. And we are actually taking an enterprise view of SBA.

Last fall, we launched our Enterprise Security Services, and we are nearly completing onboarding the program offices, where there were previously stovepipes.

So we have taken not little steps; we have taken some very big steps to get our arms around what is going on at SBA through the entire technology stack for our cybersecurity to make sure that that data is protected.

Senator CARDIN. I would ask that you keep our staff updated as to the progress you are making and complying with those concerns. I would appreciate that.

Ms. ROAT. Will do.

Senator CARDIN. Dr. Romine, you mentioned the Cyber Framework, NIST's Cyber Framework. I would be interested in how that is tailored towards small businesses and making it more useful for small businesses.

Also, if you could, as you know, Congress passed the Small Business Cybersecurity Act. It was signed into law August of last year. I understand the implementation is not what—it would be unrealistic to expect that it is fully implemented, but if you could give us an idea of how you are implementing those requirements, I would appreciate it.

Dr. ROMINE. Thank you, Senator.

First, let me take the opportunity to thank you for your recent visit on Monday to NIST. We are really grateful for the interest that you display in the Institute.

With regard to the Cybersecurity Framework, I would like to point out that during the development of the framework, we sought input from a very wide array of stakeholders and potential stakeholders, including small businesses, and we strove mightily to ensure that the Cybersecurity Framework as a framework was scalable across sectors, up and down the supply chain, and from large to very small businesses. So we tried to keep it in plain language.

We focused on just the five functions of identify, protect, detect, response, and recover, and tried to give a common lexicon so that people could discuss cybersecurity posture and their cybersecurity requirements with vendors, for example.

So we feel that we have anecdotal evidence that many small businesses are adopting the framework in whole or in part to either

begin a cybersecurity risk management program for their company or to augment and buttress one that already exists.

With regard to the Act that you mentioned that specifically calls on NIST to provide more support for small businesses, I just want to reiterate that we rolled out just a few weeks ago what we call the "Small Business Cybersecurity Corner," which is a website that is dedicated to providing as much useful information to small businesses as we possibly can. This includes resources from NIST but also resources from our other Federal partners as well as from nonprofit organizations that may have useful content that they can provide for small businesses to help manage their cybersecurity risk.

Senator CARDIN. Thank you.

Chairman RUBIO. Senator Shaheen.

Senator SHAHEEN. Thank you. Thank you both very much for being here and what you are doing to help small businesses.

Ms. Roat, last week, we had a hearing on Chinese industrial policy, and one of the questions that I asked one of the witnesses had to do with what SBA is doing to help small businesses deal with the cyber threat, whether it is from the Chinese or others.

You just laid out very clearly what is happening internally with controls at the SBA, but can you talk about what else SBA is doing to help those small businesses deal with cyber threats? Because, unfortunately, one of our witnesses at that hearing said that the SBA really is not doing very much and that they need to step up the game in order to help small businesses deal with an issue that is a huge challenge.

Ms. ROAT. So I am aware of the training that the SBDCs are offering. In some of the programs last fall, I reviewed some of their materials, and the training runs from very basic cybersecurity, things that you should be doing as a small business, and then stepping into a little bit more detail. So they are providing some of that training.

I cannot answer if they are telling people specifically do not buy these products or do not buy this software. That, I do not know, but I have seen some of the materials and that they are training those small businesses.

Senator SHAHEEN. Is there further discussion about what else either the SBDCs or other arms, other ways in which the SBA can help small businesses?

Ms. ROAT. I think through our partnership with DHS, the SBDC—again, I mentioned earlier the cyber plan that has been put together that is in final clearance. I think that that will go a long way to education, the role of the SBDCs and what they need to do, not just offering basic training, but what other things they should be doing to help address exactly what you are talking about.

Senator SHAHEEN. Have you thought about partnering with other agencies, whether it is Homeland Security, with the plan?

I know last year, there was a requirement that in order to bid on certain defense contracts, there had to be certain cybersecurity measures in place for small businesses, and that presented a huge challenge to many of our businesses in New Hampshire because they just did not have the capacity, the resources to get the help they needed in order to quality.

Has the SBA thought about partnering with DoD or other Government agencies that are requiring certain cybersecurity protections in order to bid for Government contracts?

Ms. ROAT. I know the program offices are working closely with other agencies on those requirements for cybersecurity as well as other things. There are a number of different groups, whether we work with DHS or DoD or others, and I know there are certifications in many of the other programs that SBA offers.

To your question specifically, how are we engaged on that, I am not sure that I have a complete answer on that——

Senator SHAHEEN. Yeah. I think——

Ms. ROAT [continuing]. As far as the certifications and the requirements.

I work with small businesses in my office all the time, and I do hear from them. I was on the FedRAMP program as the director, and I heard from many small businesses about the requirements around FedRAMP and security and cloud and how they get their applications to the cloud and the security requirements and should they be partnering with an AWS and a Microsoft and those big cloud providers, for their applications. I understand some of the challenges that they are having because they have brought those to me specifically when I was on the FedRAMP program.

Senator SHAHEEN. Well, thank you. It is an area that I think we should be looking at ways in which we can be creative and provide more assistance because it is clearly needed.

Dr. Romine, one of the entities that exists that helps small businesses—and you mentioned that in your written testimony—is the Manufacturing Extension Partnership. They have done a great job in New Hampshire with providing assistance, whether it is around cyber issues or in other ways, manufacturing processes with our businesses, and yet it is one of those programs which is consistently recommended by this Administration to be eliminated.

So can you talk about the importance of maintaining the MEP programs and what kinds of things they do to help business?

Dr. ROMINE. Certainly. Thank you for the question.

From our perspective, the MEP program is a really effective means of spreading the word on many different aspects of what my laboratory works on and most particularly in cybersecurity. So we have collaborated with MEP to provide additional guidance specifically related to the previous question, which is how to satisfy the requirements the Department of Defense has in pointing back to our guidance, Special Publication 800–171, which is the protection of controlled unclassified information. So there is additional guidance that helps to clarify for small businesses what they can do that is being distributed through the MEP programs.

With regard to the program itself, if Federal funding should be suspended—and that is something that, of course, is up to Congress and the Administration to work out, and I have no purview to speak on that score, but the States, as you know in your home State, also provide significant funding to those MEP centers. So although they might be required to reduce their scope, I think they would still continue.

Senator SHAHEEN. I would just correct you on New Hampshire.

Dr. ROMINE. All right.

Senator SHAHEEN. While we provide some support to the MEP program, without the Federal support, I think it is very unlikely that our program would continue.

Dr. ROMINE. Okay. All right.

Senator SHAHEEN. Thank you.

Thank you, Mr. Chairman.

Chairman RUBIO. Thank you.

Just as a follow-up to both of you, last February, we heard from the Director of the FBI before the Senate Intelligence Committee in an open hearing, and he discussed how smartphones made by Chinese government-owned companies and -backed companies like ZTE and Huawei—and this is a quote from him—have the capacity—this is a quote—"capacity to maliciously modify or steal information."

Then in the 2019 NDAA, the National Defense Authorization Act, it restricted the Federal Government's use of products manufactured by Chinese-based technology firms for substantial or critical components of any systems or as critical technology.

Can you discuss a little bit about what the Federal Government is doing to ensure that not only are we not using these products, but that we are also cautious against white labeling, which is basically the buying of technology parts from one of these companies where they are just not labeled as manufactured by one of these companies? They put a generic label on it, sometimes even their own label, and we are concerned because sensitive government work and essential government work in America, we rely heavily on the private sector and so if they are compromised with the existence of this technology, be it in routers or handheld devices or what have you, a potential liability for the whole system, what are we doing to address that particular component?

Dr. ROMINE. Thank you, Mr. Chairman. I am happy to address that question.

Although NIST has no role in specifying a specific nation state or other threat that is directly coming from a specific country, we do have an active program, an ongoing program in supply-chain risk management. This is the kind of guidance that we put out in consultation and collaboration with other Federal agencies on principles and practices that organizations can use to try to ensure that the equipment they purchase has the integrity that they expect it to have by ensuring, to the extent practicable, the supply chain of that product or service.

Chairman RUBIO. Senator Ernst.

Senator ERNST. Thank you, Mr. Chair, and thank you to our witnesses for being here today as well.

I am excited. First, Ms. Roat, I want to congratulate you on the progress that you and your team have made to improve cybersecurity capabilities and protect the valuable personal information of millions, and that is just so far. We still have work to do, but congratulations. Thank you so much.

Now that the Small Business Administration has caught up, what are you viewing as tomorrow's top cybersecurity challenges, and what can we do to combat those emerging threats?

Ms. ROAT. Like you said, Senator, we have come a long way over the last 2 and-a-half years, and while we have built the foundation,

we have put some walls on what we have done, we are continuing to build out our house around cybersecurity.

We are actually a leader across the Federal Government now in the tools and the capabilities we have. We have been pilots for DHS on their CDM and their tech programs. We are going to continue to build on that and really continue to drive that innovation in our cybersecurity practices so they are not waiting on somebody else. We are using those tools that are using artificial intelligence that are really applying machine learning, so that we understand what is in our environment, where our data is going, how it is moving across the organization, building in things like SD–WAN across our application and building security in through our entire technology stack.

We are continuing to work with our program offices. While we still have legacy systems in our environment and we are continuing that work, our modernization path is taking us, looking at the enterprise as a whole, where previously it used to be in stovepipes, so that as we are looking at our data, how is our data being used, how is it moving across the organization, who is using it, both within the agency and externally with our partners.

So next steps around cybersecurity are continuing on that path with our data strategy, getting our arms around our data, making sure we know exactly where it is, who is using it, and putting those role-based access controls around all of that.

Senator ERNST. Yes. Thank you for that.

I am not sure if Senator Shaheen had mentioned it, but yesterday we had a subcommittee in Armed Services on emerging threats and capabilities. The focus of our subcommittee was artificial intelligence and machine learning and that type of technology. So it just even discussed how can we best utilize and leverage different departments, different agencies within the Federal Government working together through research and development and then applying those technologies. Do you see that that synchronization could possibly exist between our agencies as each of you look into cybersecurity and artificial intelligence?

Ms. ROAT. So I think a lot of that activity through the CIO Council is going on right now around a lot of the artificial intelligence, a lot of those things really looking at how that can be applied. Zero-trust networks is one of those things as well. But through the CIO Council, the committees under the CIO Council are actually—the information sharing is going on, the pilots, the testing, and gathering that.

So through the CIO Council—let me put a plug in for them.

Senator ERNST. Yeah, very good.

Ms. ROAT. But there is a lot of work already under way in that area.

Senator ERNST. Very good. Well, I appreciate that.

Dr. Romine, thank you so much for being here as well. Those new small businesses and small businesses that have gained new capabilities such as access to rural broadband may be especially vulnerable to cyberattacks.

I come from a rural area. I know this is a concern that so many of our businesses do have. What steps can we take to ensure that these types of small businesses that are newly exposed to those

cyber threats are equipped with the tools and the resources they need to be cybersecure as quickly as possible?

Dr. ROMINE. Thank you, Senator.

I think the best way I can address that is to again talk about the urgency of getting the word out on the importance of managing cybersecurity risk at all businesses, at all levels, regardless of size or location.

That word, we are trying to spread more effectively, and this hearing, I am grateful is going to be doing that in part. We get a spotlight on this issue.

The resources that we are making available through the Small Business Cybersecurity Corner can be a good starting point, the NIST website that we have stood up to specifically address the concerns of small business in the cybersecurity arena.

So I would just point to that and to the Cybersecurity Framework as a flexible way of helping initiate the management of cybersecurity risk in any organization.

Senator ERNST. Very good. We just need to ensure that they know the path forward and how to make sure that they are secure and that their clients or customers are secure as well, so thank you.

Thank you very much to our witnesses, and thank you, Chair and Ranking Member.

Chairman RUBIO. Thank you.

Senator Rosen.

Senator ROSEN. Mr. Chairman, thank you for being here today and for the work that you are doing.

I was an original cosponsor of the NIST Small Business Cybersecurity Act. I am very happy it was passed into law last session.

So can you tell me how you think the situation has improved since we have put that bill in?

I would also like to know—you said we have the website up, and there are on-ramps for small businesses. Do you have the data or the numbers of the amount of usage of those websites?

Dr. ROMINE. Thank you for the question.

We do not yet. The website is relatively new. We will be tracking the number of times that it is visited and downloads of any documents that we have, not to origin, but just in terms of numbers of downloads.

Senator ROSEN. I think it would be really helpful if you provided us, those analytics, even with region of the country or where it is, because if that website is not getting utilized enough, then what is our challenge to be sure that people know that they have this way to use it as an on-ramp?

Dr. ROMINE. Absolutely right. I appreciate that.

I think we still have a lot of work to do to get the word out. As I said, the website has been stood up for just a few weeks, and so it is very early days yet, but our goal is to ensure that we do the maximum that we can to ensure that there is awareness of the site.

Senator ROSEN. How are you spreading the word?

Dr. ROMINE. We are doing that in part through—again, this is very, very early days.

Senator ROSEN. Uh-huh.

Dr. ROMINE. But we are doing this in part through our partnership with SBA. We are doing it through our partnership with the Manufacturing Extension Partnership program within NIST. So we have collaborated on resources to help support small businesses in some of the requirements that the Department of Defense has in their acquisitions requirements.

So we are going to leverage that because that is a nationwide system that is designed to get the word out to small businesses, specifically manufacturers, but we think it is broadly applicable.

We have a number of people who are subscribers to information services to keep abreast of activities that are going on in cybersecurity, and then we have a huge number of private-sector partners with whom we work collaboratively on a regular basis. We want them to get the word out as well.

Senator ROSEN. I would hope you consider partnering with our Chambers of Commerce, and particularly in the States, maybe each governor probably has an office of small business, and that through our State legislatures, we would be able to disseminate the information.

Dr. ROMINE. Absolutely.

Senator ROSEN. I think that would be something terrific.

Senator ROSEN. And as we disseminate this information at NIST, we are sure that we have a well, robust, trained cybersecurity workforce. What kind of investments do you think we can make in helping provide the people pipeline and trying to promote good business practices there?

Dr. ROMINE. NIST is privileged to lead the interagency activity, the National Initiative for Cybersecurity Education, or NICE, and that is dedicated to strengthening the pipeline of highly qualified workers in the cybersecurity arena, both cybersecurity-educated workers who we expect to work in the cybersecurity field as well as a greater understanding of the importance of cybersecurity and some of the elements in a generally more educated workforce.

Senator ROSEN. Who are your partners with that in our States that we can point to?

Dr. ROMINE. Let us see. In the State, I know that we are——

Senator ROSEN. How are we getting the information?

Dr. ROMINE. I know that we are working with a lot of other Federal agencies in that space. We have, again, a pretty active website of available activities. We have contractors who have developed a website that is specifically designed to display where jobs are available across the Nation and where there is a concentration of workers.

Senator ROSEN. If it does not get down to individuals who want to seek training for these things, the problem I see in a lot of these is we pass these frameworks, but then the information is not really—it is not disseminated to people who really need it.

Dr. ROMINE. Right.

Senator ROSEN. School guidance counselors, college guidance counselors, career and technical education, apprenticeships.

So it is great that we have these websites. It is great that you have all this information and you have some partners, but if it is not ultimately sent out to everyone in a way that we can turn that into action, then it is not very useful.

So that is why I am hoping we are going to see some future analytics from you that will point us as to how we can educate our schools, guidance counselors, and all the like to prepare students for these kinds of jobs.

Dr. ROMINE. Right. We certainly do intend to be more aggressive about getting the word out, and we routinely interact with both the U.S. Chamber of Commerce as well as local Chambers of Commerce in some of the dissemination of information that we have.

Senator ROSEN. Thank you.

Chairman RUBIO. Senator Markey.

Senator MARKEY. Thank you, Mr. Chairman, very much.

There is a Dickensian quality to the internet. It is the best of liars and the worse of liars simultaneously. It can enable. It can ennoble. It can degrade. It can debase. It all depends upon how it is used.

So we have a situation where IoT, the Internet of Things, is also IoT, the Internet of Threats. You just cannot separate them out unless you are realistic and want to build in the protections, the safeguards to ensure that the vulnerabilities are minimized.

Last Congress, I introduced a bill called the Cyber Shield Act, which I will introduce again this year. I am doing it with Congressman Lieu, over in the House, and what the bill would do is to create an advisory committee on cybersecurity, experts from academia, industry, small businesses, consumer advocacy communities, and the public to create cybersecurity benchmarks for IoT devices, such as baby monitors, cameras, toasters, refrigerators, toys, et cetera.

The IoT manufacturers can then voluntarily certify that their products meet these industry-leading cybersecurity and data security benchmarks and display the certification in public, like Energy Star. There it is. Now for cyber, you have the same kind of information.

My bill would reward manufacturers adhering to the best data security practices while also ensuring small businesses can make more informed choices. They are going to need information so they can make the right choice.

Ms. Roat, how could we help reward small IoT businesses that are adhering to and investing in the best cybersecurity and data security protections?

Ms. ROAT. So as we are working with the small business, I know the Small Business Development Committees, the SBDCs, are working with small businesses to try to educate them on what they need to do.

I had read the bill on the Cyber Shield. I think one of the challenges around that is making sure that it is kept up to date and that people want to volunteer to participate in that to get the information out, so that the small businesses in turn know how to use and get to that information. And that is critically important.

But that education piece and the communication and the constant facilitation, not just providing, say here is something, go look at it, but really facilitating that discussion with the small businesses so they really understand and truly understand what it really means and what those threats are.

You said IoT, the Internet of Threats, but how does the small business not just—how do you get through to them to really understand what that threat factor is?

Senator MARKEY. I appreciate that. I do not know a lot about electricity or other, but I know what Energy Star is. So I am just an ordinary consumer trying to figure it out, and I am kind of saying, "Okay. That is a voluntary standard, and I will trust that." If I find out I do not trust it, next time I am in the store, I am just going to say that was a piece of crap that I got sold, just so you know, sir or ma'am. So that is kind of how I view this. It is just information.

Then one of the problems in cybersecurity is you do have to keep updating it.

Ms. ROAT. Mm-hmm.

Senator MARKEY. It is just not a static thing. So the industry that is selling the devices should have a responsibility to keep updating, so that the consumer or the small business knows that this is a 2019 standard, not a 2016 standard, and there it is, a 2019 five-star or a four-star or a three-star. But then you can choose. If you do not want to pay for the five-star, fine, but you understand that at a three-star and two-star, you are taking a risk.

Would you think that would be helpful to small businesses to have that kind of information, especially the ones that have a little bit of—maybe they have got a 23-year-old on staff who can tell them what it means, you know, making the decision.

[Laughter.]

Ms. ROAT. I think it could be helpful, especially for those small businesses where you have folks that may have that 23-year-old, but that 23-year-old really, again, needs to understand what—like the Energy Star, what that really means and what the importance of it is.

Senator MARKEY. Right.

Ms. ROAT. So having something like that definitely would be useful for the small businesses because they could have a list and say okay, this, this, this, and this is what I need.

Senator MARKEY. Right. And I agree with you. I mean, it is a way of not having a mandate, but yet it is voluntary. You do it or you do not do it. You do not even have to do it. You just have your product out there without a cybersecurity, but when you are trying to buy a car and it says five stars for safety, four, three, two, you can ask extra questions. If you have a 3-year-old, you can ask extra questions. What is the security that is missing in this vehicle? If you want to just go discount, you can do it, but you are taking the risk, in other words. It is right there for you to see.

Having the information ultimately, from my perspective, is going to be something that it drives the whole industry because people will gravitate towards excellence. They will gravitate towards security and especially every day that there is another breach, and you are now purchasing something for your company, your small company, that could help to avoid something that happened at Equifax or TJ Maxx or something where their whole system went down, and then you find out later, they were using a three-star safety system, which in a lot of instances, that is what the big companies were using.

So you really want to make this a virtuous technological competition, and then those that are doing the best let you know. And I think then people would gravitate towards it.

I am hoping I can work with the community towards achieving that goal.

Thank you, Mr. Chairman.

Chairman RUBIO. Thank you.

I want to thank both of you.

Do you have any further questions?

[No response.]

So thank you both for being here. I appreciate it. We are grateful for your testimony and for answering our questions.

We will transition to the second panel as I begin to introduce them, so thank you. I guess we will have to get one more chair up there.

So let me introduce the second panel as they come up and get ready. Karen Harper of Cambridge, Massachusetts, is the president of Charles River Analytics, Inc., which uses international property to serve Government and private clients. Ms. Harper is also the principal scientist at Charles River, specializing in developing unmanned systems and other innovative products.

Elizabeth Hyman is an executive vice president at CompTIA, here in Washington, D.C. She has extensive experience with IT policy from working with Lenovo and the Consumer Technology Association. Her role in government affairs for this technology association began by working for the Attorney General, the Vice President, and the Office of the U.S. Trade Representative.

Stacey Smith is the president and CEO of the Maryland Cyber Alliance.

Senator CARDIN. You can tell by her scarf.

Chairman RUBIO. You can tell by the scarf, he says.

The Maryland Cyber Alliance or CAMI. Is that right? At CAMI, Ms. Smith works with business partners, cybersecurity professionals, and Maryland government to create cybersecurity jobs. Previously, she was a small business owner and served as the Cyber Community Manager for the Maryland Department of Commerce.

Thank you all for being here with us today.

Ms. Smith, we will begin, if you have a statement for us.

STATEMENT OF STACEY SMITH, PRESIDENT AND CEO, CYBER ASSOCIATION OF MARYLAND, INC.

Ms. SMITH. Thank you.

As you mentioned, I am Stacey Smith, the president of the Cybersecurity Association of Maryland, Incorporated, or CAMI, as we are known, for short. Our organization is a statewide, nonprofit organization based in Baltimore City, and we are with a mission of job creation and sales generation through Maryland's cybersecurity industry.

Our members include almost 450 of Maryland's cybersecurity product and service companies, many of which are small companies focused on helping small businesses be more cybersecure.

In 2017, the Better Business Bureau conducted a national study and published the "State of Cybersecurity Among Small Businesses

in North America" report. Eighty-five percent of the businesses surveyed had 50 or fewer employees and were in various industry sectors, including retail, construction, financial, manufacturing, real estate, health care, and others.

The research found that small businesses are becoming more aware of cyber threats and are taking proactive steps to enhance their cybersecurity. In fact, 9 out of 10 said they have some form of cybersecurity in place, with the most common being antivirus and firewalls.

But that is not nearly enough to ensure a business is safe from today's advanced cyber threats. As a result, they leave themselves vulnerable and may even lose more through a cyberattack than they would have spent implementing cybersecurity protections to prevent them.

If small businesses are more cyberaware than ever, why are not they doing more to protect themselves, their data and their customers?

The BBB's research found that companies are ill-equipped, primarily due to a lack of resources, including funds, and the lack of knowledge—what to do, who to consult or hire.

Here are a few real-world cyberattack examples provided by some of our members.

A small marketing firm in Baltimore was hit with a ransomware attack. Everything on their server, including client documents, financial spreadsheets, and the project tracking software at the core of their day-to-day business, were locked and held for ransom.

Hackers had used automated bots to search the internet for vulnerable servers without the necessary security controls. When the bots reached the agency's server, they hit pay dirt.

The agency reached out to a Maryland cybersecurity company that restored their systems, and 317,000 files had to be painstakingly restored. Two days of client work were lost. It took 4 days to fully restore everything, and the business spent thousands of dollars to mitigate the situation.

In another example, the CFO for a small Maryland construction company fell target to an email phishing scam. He received a message from what looked to be one of their regular payees asking him to update wire information and transfer money. He did so.

Seeing a vulnerable target, the hacker sent another message that ultimately allowed access for a ransomware attack through which the company's files were locked until the company paid the ransom money.

In total, the company lost almost $200,000 through the wire transfer, ransom payment, and cost for a Maryland cybersecurity company to completely restore and rebuild their network.

Lastly, another recent example, a small organization noticed anomalies affecting the CEO's electronic calendar and documents and reached out to a Maryland legal firm for help. The firm's data security breach response team's investigation revealed that the organization's recently fired head of Information Technology had hacked back into the organization's systems and deleted key events and documents of the CEO and ex-filtrated electronic personal health information of thousands of Marylanders.

The U.S. Attorney's Office and FBI were notified. The hacker was charged and sent to prison. The legal firm helped the organization notify affected individuals.

Had these businesses had proper protections and employee training in place, it is possible that the cyberattacks could have been prevented or mitigated, saving them from immeasurable stress; time, production and financial losses; and even reputational damage.

But, as previously mentioned, small businesses often do not know what help they need or where to go for help, and the fear of the cost keeps many of them from investing in cybersecurity before they are faced with a cyberattack.

Luckily, for Maryland businesses, CAMI exists to connect them to companies within our State with answers to their questions and products and services they need to be cybersecure.

They can connect online through our directory of Maryland cybersecurity providers. They can also attend events, including our upcoming Maryland Cyber Day Marketplace, to connect face-to-face with local cybersecurity companies.

If funding is the issue, our State legislators passed a nationally unique bipartisan bill in 2018, making it more affordable for businesses to be cybersecure. The bill provides a tax credit for Maryland businesses with 50 employees or less for 50 percent of what they spend on cybersecurity products and services purchased from a qualified Maryland cybersecurity seller, up to $50,000 annually for that tax credit.

In 2019, we have $4 million to award in tax credits to small businesses through this program.

Our organization has partnered with the Maryland Department of Commerce, the Better Business Bureau of Greater Maryland, Regional Manufacturing Institute of Maryland, Maryland Manufacturing Extension Partnership, and others to make small businesses aware of the tax credit program to incentivize them to be proactive rather than reactive in their efforts to be cybersecure.

This local bill provides a tool for Maryland cybersecurity companies to generate local sales, grow, and ultimately add jobs as they do so, and it incentivizes Maryland businesses to purchase the cybersecurity products and services they need, thus ensuring a more cybersecure business environment in Maryland.

Thank you for the opportunity to testify, and I am happy to answer any questions.

[The prepared statement of Ms. Smith follows:]

Testimony Before the U.S. Small Business & Entrepreneurship Committee
Cyber Crime & Existential Threat to Small Businesses
Stacey Smith, CEO, Cybersecurity Association of Maryland, Inc. (CAMI)

Thank you. I am Stacey Smith, CEO of the Cybersecurity Association of Maryland, Inc., or CAMI for short. CAMI is a statewide, nonprofit organization based in Baltimore with a mission of sales generation and job creation through Maryland's cybersecurity industry. Our members include almost 450 of Maryland's cybersecurity product and service companies, many of which are small companies focused on helping small businesses be more cyber secure.

In 2017, the Better Business Bureau conducted a national study and published the "State of Cybersecurity Among Small Businesses in North America" report. 85% of the businesses surveyed had 50 or fewer employees and were in various industry sectors including retail, construction, financial, manufacturing, real estate, healthcare and others.

The research found that small businesses are becoming more aware of cyber threats and are taking proactive steps to enhance their cybersecurity. In fact, 9 out of 10 said they have some form of cybersecurity in place with the most common being antivirus and firewalls.

But that's not nearly enough to ensure a business is safe from today's advanced cyber threats. As a result, they leave themselves vulnerable, and may even lose more through a cyberattack than they would have spent implementing cybersecurity protections to prevent them.

If small businesses are more cyber aware than ever, why aren't they doing more to protect themselves, their data and their customers? The BBB's research found that companies are ill-equipped primarily due to a lack of resources, including funds, and the lack of knowledge – what to do, who to consult or hire.

Here are a few real cyberattack examples provided by some of our members:
A small marketing firm in Baltimore was hit with a ransomware attack. Everything on their server including client documents, financial spreadsheets and the project tracking software at the core of their day-to-day business were locked and held for ransom. Hackers used automated bots to search the internet for vulnerable servers without the necessary security controls. When the bots reached the agency's server, they hit pay dirt. The agency reached out to a MD cybersecurity company that restored their systems and 317,000 files had to be painstakingly restored. Two days of client work were lost. It took four days to fully restore everything, and the business spent thousands of dollars to mitigate the situation.

In another example, the CFO for a small MD construction company fell target to an email phishing scam. He received a message from what looked to be one of their regular payees asking him to update wire information and transfer money. He did so. Seeing a vulnerable target, the hacker sent another message that ultimately allowed access for a ransomware attack through which the company's files were locked until the company paid the ransom money. In total, the company lost almost $200,000 through the wire transfer, ransom payment and cost for a MD cybersecurity company to completely restore and rebuild their network.

Lastly, another recent example - a small organization noticed anomalies affecting the CEO's electronic calendar and documents and reached out to a MD legal firm for help. The firm's data security breach response team's investigation revealed that the organization's recently-fired head of Information Technology had hacked back into the organization's systems and deleted key events and documents of the CEO and exfiltrated electronic personal health information of thousands of Marylanders. The US Attorney's Office and FBI were notified. The hacker was charged and sent to prison. The legal firm helped the organization notify affected individuals.

Had these businesses had proper protections and employee training in place, it is possible that the cyberattacks could have been prevented or mitigated saving them from immeasurable stress; time, production and financial losses; and even reputational damage.

But as previously mentioned, small businesses often don't know what help they need or where to go for help, and the fear of the cost keeps many of them from investing in cybersecurity before they are faced with a cyberattack.

Luckily, for MD businesses, CAMI exists to connect them to companies within our state with answers to their questions and products and services they need to be cyber secure.

They can connect online through our directory of MD cybersecurity providers (www.MDcyber.com/listings). They can also attend events, including our upcoming MD Cyber Day Marketplace, to connect face-to-face with local cybersecurity companies.

If funding is the issue, our state legislators passed a nationally unique BIPARTISAN bill in 2018 making it more affordable for businesses to be cyber secure.

This bill provides a tax credit for MD businesses with 50 employees or less for 50% of what they spend on cybersecurity products and services purchased from a Qualified MD Cybersecurity Seller - up to a total tax credit of $50,000 annually. In 2019, we have $4 million to award in tax credits to small businesses through this program.

Our organization has partnered with the MD Department of Commerce, the Better Business Bureau of Greater Maryland, Regional Manufacturing Institute of Maryland, MD Manufacturing Extension Partnership and others to make small businesses aware of the tax credit program to incentivize them to be proactive rather than reactive in their efforts to be cyber secure.

This buy-local bill provides a tool for Maryland cybersecurity companies to generate local sales, grow and ultimately add jobs as they do so, and it incentivizes MD businesses to purchase the cybersecurity products and services they need, thus ensuring a more cyber secure business environment in Maryland.

Thank you for the opportunity to testify. I am happy to answer any questions you may have.

stacey@MDcyber.com, (443) 844-0047, www.MDcyber.com

Chairman RUBIO. Ms. Hyman.

STATEMENT OF ELIZABETH HYMAN, EXECUTIVE VICE PRESIDENT, COMPTIA

Ms. HYMAN. Chairman Rubio and Ranking Member Cardin, on behalf of the Computing Technology Industry Association, CompTIA, thank you so much for having me here today.

CompTIA is the leading voice and advocate for the $1.6 trillion U.S. information technology ecosystem and the more than 11.5 million IT professionals who design, implement, manage, and safeguard the technology that powers the world's economy.

As we have discussed, small businesses are the backbone of our economy, but they are fertile targets for cybercriminals looking to exploit vulnerable defenses. Small businesses have fewer employees and resources than large enterprises and because of this have less to invest in cybersecurity.

CompTIA works with small businesses and customers on a daily basis, and we are committed to ensuring that they are educated on and protected from the threats that they are facing.

At one time, cyberattacks were considered just an IT problem, and that is certainly not the case anymore. Cybersecurity issues have grown in size and scope, becoming more sophisticated, harder to detect, and more widespread.

As Senator Cardin has already noted, according to the 2018 Verizon Data Breach Investigation Report, 58 percent of breach victims were characterized as small businesses. Research by Cybersecurity Ventures estimates that by 2021, cybercrimes will cost $6 trillion per year.

While improved cybersecurity is needed across the board, small companies are the ones with the steepest challenge. According to our research, 62 percent of small businesses have internal resources focused on security compared to 91 percent for medium-size businesses and 96 for large firms. Understanding the problems facing small businesses is only part of the challenge.

We must also aggressively put forward solutions and enlist the help of public partners like the Small Business Administration and NIST to help address these challenges.

We must focus on improving three key elements of modern security. The first are technology tools. SMBs need advice and guidance on what a modern security toolset should include. This can range from data loss prevention software to more proactive tools and methods, such as penetration testing which assesses the strength of a defense system.

Secondly, focus is needed on helping small businesses develop business processes that reflect how to build security policies and establish proper enforcement. This will include internal operations as well as relationships with outside suppliers of services or partners. A great place to start in this discussion is to develop metrics to track the effectiveness of security programs and processes, such as, for example, tracking results from phishing expeditions.

Lastly, we need effective employee education. Many small businesses have a small team or a solo IT professional who needs to have a solid foundation in security skills, sufficient specialized expertise in a few key areas, and then the ability to work with an

outside partner, such as a managed security services provider, when deep expertise is called for.

CompTIA is one of several vendor-neutral certifying bodies that offer certifications, high-stakes exams, that are ANSI- and ISO-accredited.

CompTIA is the market leader, having certified more than 2 million people in more than 100 different countries. There are many ways our certifications can help support small businesses and enhance their cybersecurity.

CompTIA's Cybersecurity Pathway includes certifications that describe the basics of IT systems, such as our IT fundamentals exam or an A-plus exam, and others that describe the technical aspects of cybersecurity, such as Security Plus, CompTIA Cybersecurity Analyst Plus, and Penetration Testing Plus.

Completion of at least IT Fundamentals and A–Plus would position a small business IT professional to successfully handle internal cybersecurity matters and oversee third-party managed security firms.

Finally, it is vital that we focus on establishing a culture of cybersecurity within any organization, including small business owners and principals. As CompTIA outlined in our white paper, "Building a Culture of Cybersecurity: A Guide for Executives and Board Members," there are six principles that all organizations can adopt on a scale that is appropriate for their business.

One, integrate cybersecurity into a business strategy.

Two, insist that the corporate structures reinforce a culture of cybersecurity, otherwise leadership is not sending the message that this matters.

Understand that employees are the biggest risks. Consider education for the employees, even considering access to company data to mitigate damage.

Focus on detection. The longer it takes to detect a data breach, the more expensive that breach becomes.

Emphasize data protection, that is, collect what is needed. Share only what needs to be shared.

And, finally, develop robust contingency plans and test them.

By working together and continuing to embrace the private-public partnership that has long benefited the cybersecurity ecosystem, we can do a great deal to help better prepare small businesses and businesses of all sizes for the cybersecurity threats they are facing.

I thank you for the opportunity to participate in the hearing today and look forward to your questions.

[The prepared statement of Ms. Hyman follows:]

CompTIA.

United States Senate Committee on Small Business and Entrepreneurship

"Cyber Crime: An Existential Threat to Small Business"

Testimony by Elizabeth Hyman, Executive Vice President, CompTIA

March 13, 2019

Introduction

Chairman Rubio and Ranking Member Cardin, on behalf of the Computing Technology Industry Association (CompTIA), thank you for having me here today. CompTIA is the leading voice and advocate for the $1.6 trillion US global information technology ecosystem, and the more than 11.5 million American information technology (IT) professionals who design, implement, manage, and safeguard the technology that powers the world's economy.[1] Through education, training, certifications, advocacy, philanthropy, market research and membership programs, CompTIA is the hub for advancing the tech industry and its workforce.

As you well know, small business is the backbone of our economy. However, our small businesses are at risk from hackers and nation states. Small businesses have fewer employees and resources than large enterprises and are fertile targets for cyber criminals looking to exploit vulnerable defenses. Our nation's small businesses need help.

CompTIA works with small business members and countless small business customers on a daily basis and we are committed to working with this committee to ensure that all business owners are educated on and protected from the threats they are facing.

Sizing Up Today's Threats

At one time, cyberattacks were just an "IT problem" that featured such nuisances as defaced websites, occasional viruses that made the lives of IT workers miserable, or the odd hacked e-mail account or two. Sometimes, individuals heard about cybersecurity problems when their credit card was compromised. Occasionally, an astute individual may have heard of a Distributed Denial of Service (DDoS) attack or news about a few obscure wily hackers who had stolen someone's identity. Traditional security approaches had the ability to manage many of these attacks.

Conditions have changed dramatically over the last five years. Our society is becoming more connected and the proliferation of IoT and other systems will only increase this trend. As CompTIA research suggests, cybersecurity issues have grown in size and scope, becoming more sophisticated, harder to detect and more widespread (see attached report on The Evolution of Security Skills). They have also increasingly been aimed at the pillars of our society: credit agencies, major retailers, government and military departments, information services and elements that underpin our democratic processes are under regular attack.

[1] www.comptia.org

To compound the threat, regular users and IT professionals alike do not always have adequate skills to protect themselves and others. In 2017, we saw the proliferation of successful "phishing" attacks that trick individuals into revealing sensitive information (e.g. passwords) or installing malware on their system[2]. In February of 2018, a company called GitHub experienced the largest DDoS attack ever recorded.[3]

It is worth noting that according to the 2018 Verizon Data Breach Investigation Report, 58% of breach victims were characterized as small businesses.[4] We have seen the trend of cyber attackers shifting their attack patterns to exploit third- and fourth-party supply chain partner environments to gain entry to target systems.[5] We need only look as far as the massive Target breach of 2013, where it is believed that hackers gained access to the Target network by successfully hacking a small business vendor to the retail giant, to appreciate the idea that we are all vulnerable to the weakest link in our digitally connected economy.[6]

The overall costs of cybersecurity compromises are enormous. Research by Cybersecurity Ventures estimates that by 2021, cybercrimes will cost $6 trillion per year worldwide.[7] This includes not only stolen money and ransom, but also the value of lost productivity and intellectual property, data theft, business disruption, reputational harm and more. As a result, many organizations are finding it difficult to keep up with the costs of protecting data and sensitive information.

The Cybersecurity Challenges for Small Businesses

Traditionally, small businesses have invested less in cybersecurity because of limited resources or the assumption that their digital assets are of less value to cybercriminals. With any form of digital data now holding some value (customer data, employee information, records relating to government clients, etc.), businesses of all sizes must view cybersecurity as a vital business expense. According to CompTIA research, only 14% of businesses with less than 100 employees feel that their current cybersecurity strategy is completely satisfactory, compared to 20% of businesses with 100-499 employees and 27% of businesses with 500 or more employees.[8] While

---

[2] APWG *Phishing Activity Trends Report, First Half 2017*, October 2017, http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf

[3] Wired Magazine, *GitHub survived the biggest DDoS attack ever recorded*, March 1, 2018, https://www.wired.com/story/github-ddos-memcached/

[4] *Verizon Data Breach Investigation Report, 2018*, https://enterprise.verizon.com/resources/reports/dbir/

[5] Accenture, "*Ninth Annual Cost of Cybercrime Study*," March 6, 2019, https://www.accenture.com/t20190305T185301Z__w__/us-en/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

[6] CNBC, "*Congress addresses cyberwar on small business: 14 million hacked over last 12 months*," April 5, 2017 https://www.cnbc.com/2017/04/05/congress-addresses-cyberwar-on-small-business-14-million-hacked.html

[7] Cybersecurity Ventures, *2017 Cyber Crime Report*, October 2017, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[8] CompTIA *2018 Trends in Cybersecurity: Building Effective Security Teams*, September 2018, https://www.comptia.org/resources/cybersecurity-trends-research

improved cybersecurity is needed across the board, small companies are the ones with the steepest challenge. CompTIA research shows that only 62% of small businesses have internal resources focused on security, compared to 91% of mid-sized businesses and 95% of large firms.[9]

The first part of the challenge is awareness of the scope of modern cybersecurity. Along with understanding that all digital assets are valuable, small businesses must understand the risk of a cybersecurity breach. According to the *2018 Cost of a Data Breach Study* by IBM/Ponemon, the average cost of a data breach to a company is $3.86 million or $148 per stolen record.[10] Although a small business may have fewer records impacted in a breach, the cumulative sum is more likely to have a catastrophic impact due to lower operating margins.

The variety of attacks has grown dramatically with the adoption of new technology models, and small businesses have low awareness of the many attack formats. For example, 64% of small firms believe that a virus could affect their business, but only 33% believe that ransomware could be a factor and 19% are concerned about a DDoS attack.[11] These other attacks take a very different form and require different forms of defense.

How the Small Business Administration Can Help Advance a Three-Pronged Defense

Small Business Development Centers (SBDCs) managed by the SBA can play an important role in helping to address the challenges unique to the cybersecurity of small businesses. To properly assist small businesses, the SBDCs should focus on improving the three key elements of modern security:

1) Technology tools
2) Business processes
3) Effective employee education

A. Improved Technology Tools: Understanding the Tools Needed

From a technology perspective, many companies have previously focused on a limited set of defensive tools (primarily firewall and antivirus). A modern security toolset expands to include protections that fits current usage, such as Data Loss Prevention (DLP), Identity and Access Management (IAM), and Security Information and Event Management (SIEM). There are also more proactive tools and methods being used, such as penetration testing that proactively assesses the strength of the overall defenses. At a minimum, cybersecurity experts advising small businesses should be familiar with the full suite of security tools available today.

---

[9] CompTIA Research Report, *2018 Trends in Cybersecurity: Building Effective Security Teams*, September 2018, https://www.comptia.org/resources/cybersecurity-trends-research

[10] IBM, *2018 Cost of a Data Breach Study: Global Overview* (by Ponemon), July 2018, https://www.ibm.com/security/data-breach

[11] CompTIA Research Report, *The Evolution of Security Skills*, April 2017, https://www.comptia.org/resources/the-evolution-of-security-skills

B. Business Processes: Measuring for Success

Building secure processes is a separate step that touches all corners of a business. Processes range from developing an incident response plan to taking simple steps to educate and test employees on basic cyber hygiene. There are many existing government resources to assist SMBs in this exercise. For example, cybersecurity advisors (also known as CSAs) are regionally-located DHS personnel who offer immediate and sustained cybersecurity assistance to prepare and protect organizations, including small and mid-sized businesses.[12] CSAs should be focused on helping small businesses understand how to build security policies and establish proper enforcement. This will include internal operations as well as relationships with outside suppliers or partners.

Regardless of the public partner, it may behoove the SBDC to consider bestowing an organizational designation similar to CompTIA's Security Trustmark (which is based on the NIST critical infrastructure cybersecurity framework) upon completion of some sort of evaluation. This designation would help the small business demonstrate to clients that they are well versed on modern cybersecurity issues and have the processes and personnel equipped to perform digital business in a secure fashion.

In addition, small businesses should have the ability to learn from each other. As has been raised in previous congressional sessions, the idea of sharing threat information between small businesses and the government is one that could add significant value to our cyber defenses.[13] Taking it one step further, the sharing of best practices on an SBA-managed platform that is populated by businesses self-reporting (perhaps in an anonymous but verified way) could prove to be an invaluable and low-cost resource for small businesses. Seeing how other similarly situated organizations have both increased their cybersecurity and responded to incidents would no doubt help to alleviate concerns for new businesses who are just getting started or existing ones facing a breach.

Ultimately, however, small businesses will need metrics to track the effectiveness of their security programs and processes. Metrics should be derived from real experience, based on private and public sector best practices and through careful coordination. It doesn't take as much time to do this as individuals might think -- real-time measurements can be created after an hour or two of coordination. If cybersecurity professionals and business leadership properly translate technical specifications and business objectives into proper communication, then organizations will have gone a long way to solving long-standing problems. Sample metrics can include improving employee/end-user education by instituting phishing and other simulations and tracking results, lowering containment times (e.g., the time between a security breach and its resolution), and response times (e.g., the amount of time it takes to restore a critical business service).

---

[12] https://www.sba.gov/managing-business/cybersecurity/top-tools-and-resources-small-business-owners

[13] H.R. 4668, Small Business Advanced Cybersecurity Enhancements Act of 2017; H.R. 3002, Small Business Cyber Training Act of 2017

C. *Effective Employee Education: Leveraging Vendor Neutral Industry-Recognized Credentials*

There is a shortage of cybersecurity workers in the United States.[14] Though a national shortage is of significance to businesses of all sizes, small businesses are at a particular disadvantage when it comes to recruiting talent. Salary sensitivity is greater when there is a demand for skilled labor. Still, there are very practical and affordable steps that SMBs can take to build expertise in all the areas that are needed for modern cybersecurity. It is especially vital to ensure that a small business IT team, which fulfill many roles, has a solid foundation in security skills, sufficient specialized expertise in a few key areas, and then the ability to work with an outside partner, such as a managed security services provider, when deep expertise is called for.

CompTIA is one of several vendor neutral certifying bodies that offer certifications that are ANSI and ISO accredited. Nevertheless, to provide greater context for this submission, we offer a description of the many tools that CompTIA presently offers.

CompTIA's Security Pathway includes certifications that describe the basics of IT systems (such as ITF+ and A+), certifications that describe the technical aspects of cybersecurity (such as Security+, CySA+, and PenTest+), and the CASP+ certification that describes the implementation of cybersecurity solutions based on organizational policies.

IT Fundamentals (ITF+) is a vendor-neutral certification that covers a broad range of knowledge and skills required of employees who have to operate within an enterprise driven by technology. Professionals operating in small- to mid-size companies many times have to bear the burden of wearing multiple hats, requiring them to have a broader range of IT skill sets. ITF+ covers topics such as IT Concepts and Terminology, Infrastructure, Application and Software, Software Development basics, Database fundamentals and cyber security. This program will ensure non-IT staff (or new IT staff) have a broad range of knowledge related to technologies and security concepts that impact them on a daily basis.

For IT support staff and other IT personnel, CompTIA's A+ and Security+ certifications are the perfect combination to ensure these staff members are well versed with the skills and abilities required to successfully perform on the job.

The A+ vendor-neutral certification covers the full gamut of knowledge and skills required to support all common hardware, devices, technologies and operating systems used in small and large corporate environments. In addition, the certification also addresses skills needed to manage basic networks, implement techniques to secure all common types of client-side devices (IoT) and understand how to best leverage cloud and virtualization technologies.

CompTIA's Security+ certification is targeted at general IT support staff who have been operating within an IT environment for approximately 2 years with a focus on security. This

[14] https://www.cyberseek.org/

certification takes a deeper dive into the challenges of securing corporate infrastructure. Professionals will need to prove competency in the areas of threats, attacks and vulnerabilities, technologies and tools used to remedy security concerns, best practices for architecture and design, identity and access management, risk management, and the importance of cryptography and public key infrastructure (also known as PKI, it is used to efficiently ensure encrypted communications can take place).

Candidates who complete the proposed pathway of all three of these certifications will have the requisite knowledge and skills to provide a broad range of IT support across many diverse platforms in small business environments while maintaining an aggressive security posture against all types of corporate threats.[15] In addition, many employers may not know what to look for when seeking out cybersecurity and IT personnel. By knowing to look for personnel that have vendor-neutral certifications, it will help to not only validate skills, but also enable employers to cross reference the skills they need with those that a certification exam is testing on.

Policy Considerations: Federal Data Breach and Notification Law

While this hearing is focused on practical steps to aid small businesses in their cybersecurity readiness, we would be remiss if we did not point out one policy consideration that we believe would be of great assistance to small businesses. Data breaches have become part of the cost of doing business. With the increasingly mobile and decentralized nature of our economy and data storage and dissemination technologies, most companies are under the umbrella of multiple state laws at all times. The need to comply with as many as 50 different state data breach notification laws is one of the drivers of the high-costs associated with data breaches. While larger organizations may be able to foot this bill and still remain in business without breaking a sweat, these are numbers that could quickly bankrupt many small businesses.

We encourage Congress to work with industry to develop a single federal standard for data breach notification. This will help alleviate these burdensome compliance costs and instead allow for SMBs to devote their time and resources to investigating and resolving the breach. The ability to do so will also better protect the consumers whose information was stolen.

Incorporate a Culture of Cybersecurity to Businesses of All Sizes

Finally, it is vital that we focus on establishing a culture of cybersecurity within any organization to help not only defend against attacks, but also help with the aftermath of an attack or breach. As CompTIA outlined in our white paper entitled, *"Building a Culture of Cybersecurity: A Guide for Executives and Board Members,"*[16] there are 6 principles that all organizations can adopt on a scale that is appropriate to their business:

- **Integrate cybersecurity into business strategy**: Senior executives and board members need to be directly involved with quantifying cybersecurity efforts across the business

[15] Those candidates wishing to progress along a cybersecurity career path can proceed to the more advanced exams of CySA+, PenTest+, and the CASP+ certification that describes the implementation of cybersecurity solutions based on organizational policies.

[16] CompTIA White Paper, *Building A Culture of Cybersecurity: A Guide for Executives and Board Members*, April 2018, https://www.comptia.org/resources/building-a-culture-of-cybersecurity-a-guide-for-corporate-executives-and-board-members

and lead the way in advancing new approaches to cybersecurity costs—and returns.

- **Corporate structure should reinforce a culture of cybersecurity**: If cybersecurity is not built explicitly into an organization, leadership is sending a message that it is not truly committed to the goal.

- **Employees are the biggest risks**: Employees may inadvertently jeopardize data, steal information for a competitor, or sell data or intelligence. Controlling access to company data can significantly improve the chances of catching this behavior before it causes devastating damage.

- **Detect, detect, detect**: The longer it takes to detect a data breach, the more expensive the data breach becomes.

- **Data protection**: Collect what is needed, share only what has to be shared. Organization needs to have flexible and adaptable approaches to protect data.

- **Develop robust contingency plans (and test them!)**: Companies must create a formal incident response team to have an end-to-end cybersecurity strategy.

SBDCs can and must play a role in imparting these principles to small businesses. We must work together as industry and government to lead by example so that company culture can truly embrace cybersecurity. SMBs must view cybersecurity as part of the broader risk management process for their business, rather than jettisoning it off as just a technology problem with a technology solution.

Conclusion

While the challenge that lies ahead of us can seem overwhelming and almost too great a burden to bear, it is one we cannot afford to ignore. By working together and continuing to embrace the private-public partnership that has long benefited the cybersecurity ecosystem, we can do a great deal to help better prepare small businesses, and business of all sizes, for the cybersecurity threats they are facing. Thank you for the opportunity to participate in this hearing and we look forward to further engagement with your Committee.

Respectfully,

Elizabeth Hyman

Executive Vice President, Public Advocacy

Chairman RUBIO. Ms. Harper.

STATEMENT OF KAREN A. HARPER, PRESIDENT, CHARLES RIVER ANALYTICS, INC.

Ms. HARPER. Good afternoon. Thank you, Chairman Rubio, Ranking Member Cardin, and members of the Senate Committee on Small Business and Entrepreneurship for inviting me to testify today on the current state of cyber vulnerabilities facing America's small businesses and the impacts that current policies, though well intended, are having on small business.

My name is Karen Harper. I serve as president of Charles River Analytics, a small research and development company employing 180 people, headquarters in Cambridge, Massachusetts, with a satellite presence in Wakefield, Rhode Island, and remote presence across the country.

Since 1983, Charles River has been delivering intelligent systems software to transform our customers' data into mission-relevant tools and solutions across Federal agencies.

For a small business, we bring an impressive array of deep technical expertise to these efforts, including artificial intelligence, sensor and image processing, human systems integration, and notably for today's hearing, cybersecurity.

Charles River has been on the cutting edge of research and development related to cyber defense for many years. Through this research, we have gained a deep understanding of the vulnerabilities of our Nation's public and private institutions, corporate entities, and private citizens. It is imperative to provide the Nation's small businesses with straightforward, pragmatic policy guidance and effective support to improve our own cyber defense systems.

Recent efforts to standardize cyber defense strategies have been implemented in the defense industry through the adoption of the National Institute of Standards and Technology, or NIST, Special Publication 800–171, to protect controlled unclassified information, or CUI, in non-Federal IT systems.

While we are small, business leaders understand the good intentions of the NIST standard. Compliance with it is currently extremely costly and overly burdensome.

The publication includes 110 IT control requirements. Many contractors are still grappling not only with the technical complexities of the requirements, but also with a lack of clarity about what actually constitutes controlled unclassified information.

This lack of clarity has been a critical concern in Charles River's NIST compliance program. Because CUI is not always clearly identified, we declared that all data on our corporate networks must be treated as CUI. It may sound simple; it has been far from it.

Our IT and software engineering teams took on the challenge of NIST compliance with gusto. However, they encountered multiple issues in their efforts. First, NIST requirements are vague. All of the 110 NIST controls can be implemented in a variety of ways, and there is a dearth of specific guidance on preferred implementation methods.

As a result, we spent approximately 800 person-hours to simply interpret the control requirements.

Second, we found that many of our customers seemed equally confused and unable to provide helpful clarification and guidance throughout Federal agencies.

Fortunately, our team is very technically savvy. After deciphering all of the NIST controls, we were able to develop a risk-gap analysis and formulate a plan of action. We then spent an additional 1,500 person-hours to implement that plan.

While we are confident that Charles River is now fully NIST-compliant, we remain unsure of how and when that compliance will be confirmed through audit.

The costs of NIST compliance are quite burdensome. We spent more than $300,000 in hardware, software, and vendor maintenance contracts. We estimate that we will spend an additional 30 percent each year on non-labor IT to maintain our compliance. Our IT staff has almost doubled in size and cost, specifically to support NIST compliance.

Now, I recognize that as an advanced software engineering company, our IT infrastructure is more complex than the average U.S. small business, and so our costs are likely higher than most. However, we cannot kid ourselves that true NIST compliance can currently be achieved at a reasonable cost to small business.

Finally, NIST compliance places a significant burden on our technical staff. Creating and maintaining compliant infrastructure drains resources from project work, resulting in less progress per dollar.

Perhaps most importantly, NIST compliance hinders and frustrates our top-performing staff, causing them to seek employment in other sectors, thus making it difficult to maintain competitive business advantage and, at the end of the day, competitive national advantage.

Given the challenge, expense, and business impacts of our NIST compliance program, we recommend improvements to the Government specification and support for its implementation across three areas.

First, we require clarity in the definition and management of CUI, both provided by our DoD customer base, but also generated by our company in the course of doing business.

Second, we require flexibility in the application of defined NIST controls. IT requirements across industry varies widely, and the implementation of NIST-compliant controls should reflect this diversity.

Finally, we require clear guidance to support proper compliance, and that guidance must be delivered in easily accessible implementation guides.

Thank you for allowing me to testify before the Committee today. I would be happy to answer any questions you may have for me.

[The prepared statement of Ms. Harper follows:]

Testimony of Karen A. Harper

Principal Scientist, President and Chair of the Board

Charles River Analytics Inc.

On behalf of the National Small Business Association

Senate Committee on Small Business and Entrepreneurship

"Cyber Crime: An Existential Threat to Small Business"

March 13, 2019

1156 15th Street, N.W., Suite 502
Washington, DC 20005
202-293-8830
www.nsba.biz

Karen A. Harper, Principal Scientist, President and Chair of the Board, Charles River Analytics Inc., Cambridge, Massachusetts

Good afternoon. Thank you, Chairman Rubio, Ranking Member Cardin and members of the Senate Committee on Small Business and Entrepreneurship, for inviting me to testify today on the current state of cyber vulnerabilities facing America's small businesses, and the negative impact current policies—intended to help mitigate cyber risks—are having on small businesses.

My name is Karen Harper, and I serve as President and Chair of the Board of Charles River Analytics, a small research and development company, employing 180 people, headquartered in Cambridge, Massachusetts, with a satellite presence in Wakefield, Rhode Island, and remote presence across the country, including Arizona, California, Florida, New York, North Carolina, Pennsylvania, and Texas.

Since 1983, Charles River Analytics has been delivering intelligent systems that transform our customers' data into mission-relevant tools and solutions to support critical assessment and decision-making across a wide spectrum of mission areas and functional domains. Charles River continues to grow our technology, customer base and strategic alliances through research and development programs for the Departments of Defense (DOD), Homeland Security (DHS), NASA, and the Intelligence Community.

For a small business, we bring an impressive array of deep technical expertise to these domains and customers, including artificial intelligence, sensor and image processing, situation assessment and decision aiding, human systems integration, human-robot interaction, and, notably for today's hearing, cyber security. Since 2013, Charles River is proud to operate as a 100 percent employee-owned company, which has set the stage for our next generation of scientific exploration, technological innovation, customer service, and growth.

I am pleased to also be here representing the National Small Business Association (NSBA), where I currently serve on the Leadership Council and the Small Business Technology Council. NSBA is the nation's oldest small-business advocacy organization, with over 65,000 members representing every sector and industry of the U.S. economy. NSBA is a staunchly nonpartisan organization devoted to representing the interests of America's small businesses which provide almost half of private sector jobs to the economy.

Small Business – Cyber-security Landscape

Small businesses face unique challenges and vulnerabilities when it comes to digital security. Business owners rely on information technology more than ever, yet the very tools that make small businesses competitive have also put them in the crosshairs of cyber attackers. The security of our online data and finances is a huge concern for America's small businesses. Early indicators from a forthcoming National Small Business Association (NSBA) survey show that 62

percent of small-business owners are very concerned that their business could be vulnerable to a cyber-attack—both in terms of being targeted by a cyber-attack as well as the potential for unnecessary regulatory burdens that could accompany efforts to stem online attacks. The level of risk for being a target of cyber-crime is high, that same data suggests that one-in-three have been the victim of a cyber-attack.

The most common type of cyber-attack, according to NSBA's data, caused a service interruption or information falsely sent out under the businesses name. Other common kind of cyber-attacks for small business are general computer hacks, stolen credit card information and website hacks. However, threats can also include attacks launched through email, SMS and voice phishing, even insider threat attacks, or in person cyber-security attacks. Small businesses are also very likely to suffer a reputational attack, where someone starts posting negative information in social media, websites, and blog posts to harm their brand and or reputation. Of the number of NSBA members who were victims of credit card theft, 13 percent said their company's entire network was compromised and for 10 percent their banking accounts were breached. Small businesses often operate on very tight profit margins and seldom carry a lot of excess cash. These losses can be devastating to businesses in those circumstances.

Small Business Operational Perspective

The forthcoming NSBA survey shows that in a technologically advanced economy, network vulnerabilities and the lack of a comprehensive cyber-security policy can completely disrupt business. The results indicate that resolving these issues is significant as well, with one-in-four saying it took them more than three days to find a resolution.

This is an incredible burden on an organization of any size, but when factoring in the fact that small businesses have limited financial and technological resources, the problem becomes compounded. Only 14 percent of small business rate their ability to mitigate cyber risk and vulnerabilities as effective.

For those owners handling it themselves, it is certainly expected that resolving incidents will require research, training, trial and error, and a great deal of time away from the core functions of the business—acting as accountant, benefits coordinator, attorney, and personnel administrator. Simply outsourcing the function is not necessarily a silver bullet either.

As a result, small businesses must become more efficient in their utilization of cyber-security methods that are designed to help mitigate the potential risks of cyberattacks. The statistics show that there is a significant amount of work to be done on part of small companies and their operational strategies.

For these reasons, NSBA is pleased that Chairman Rubio will be introducing the Small Business Cyber Training Act of 2019, which would require Small Business Development Centers

(SBDCs) that have received grants from the Small Business Administration (SBA) to develop a counseling program and authorizes the SBA to fund that training. If passed, it will increase access to cyber-security expertise for small businesses and improve the safety of their data collection and storage methods. These additional resources from the SBA through the SBDCs—which many business owners utilize in their communities—may further improve cyber-security practices across all industries.

One of the most popular responses on why small businesses do not allocate financial resources to threat mitigation is that they feel they do not store any valuable data. This is a misconception on what constitutes valuable data – email, phone numbers, billing addresses may be viewed as not valuable information to the small business, but to a cyber-criminal, these are very valuable and effective data points that can be used for malicious purposes. Although small-business owners are becoming increasingly tech savvy, limited resources and knowledge still leave many vulnerable to cyber-threats.

NSBA has long urged Congress to move forward on establishing streamlined guidelines and protocols to ensure the protection and security of our online data and financials, but cautions against a knee-jerk reaction that would unfairly place a disproportionate burden on America's smallest firms. Legislation to enhance America's cyber-security should provide clear, simple steps for companies to follow when their data is breached and must balance the need for greater information sharing with privacy rights.

Charles River Analytics

Charles River has been on the cutting edge of Research & Development (R&D) related to cyber defense for many years, working with science and technology groups within the DOD, DHS, and the Intelligence Community, to develop better ways to identify and defend against cyber-attacks.

For example, working for DARPA (the Defense Advanced Research Projects Agency), we have created tools to process millions of pieces of malware and have seen firsthand how much malware is out there, how sophisticated it often is, and how it changes over time to avoid detection. We have worked with the Air Force Research Laboratory (AFRL) to develop tools that use advanced machine learning techniques to predict changes in malware, so we are better able to detect novel malware, but are not yet able to predict all of the ways that sophisticated attackers change their attacks. Finally, we are currently finishing up a project with IARPA (the Intelligence Advanced Research Projects Agency) where we are attempting to predict specific types of cyber-attacks. As part of this effort, we have seen just how many attacks there are, both random and targeted, against small and medium-sized businesses, and how little information there is to tip cyber defenders off to pending attacks before the damage is done.

Through this research experience, Charles River has gained a deep understanding of the vulnerabilities of our nation's public and private institutions, corporate entities (including small

businesses across all industries), and private citizens. We also understand the value of the data at risk to a cyber attack. Whether it is personally identifiable information (PII) of the private citizen, the proprietary and confidential data of companies and institutions, or the data that supports and protects our national security, the potential of compromise to this data can be devastating to the individual, organization, and the nation as a whole. Therefore, it is imperative to provide the nation's small businesses with straight-forward, pragmatic policy guidance and effective support to dramatically improve our own cyber defense systems.

National Institute of Standards and Technology (NIST)

Recent efforts to promote and standardize cyber defense strategies have been implemented in the defense industry, through the adoption of the National Institute of Standards and Technology (NIST) Special Publication 800-171 requirements to protect Controlled Unclassified Information (CUI) in non-federal IT systems. All DOD contractors that process, store or transmit CUI must meet the Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards or risk losing our DOD contracts.

The NIST standard is broken down into fourteen areas. In each of these areas, DOD contractors must adhere to specific security requirements. The rule requires contractors to notify the DOD CIO within 30 days of contract award of any security requirements not implemented at the time of contract award. Often, when the government comes up with new compliance regulations, it becomes a headache for businesses, especially small ones, to oblige in a timely manner.

While small-business leaders such as myself, understand the intentions of the NIST SP 800-171 standard to protect the cyber vulnerabilities we all face, compliance with NIST SP 800-171 is extremely costly and overly burdensome, particularly for small businesses. The publication includes 110 (!) IT control requirements, many of which require highly complex solutions. As a result, many contractors are still grappling with the complexities of NIST SP 800-171, as well as other aspects of DFARS, such as what actually constitutes "Controlled Unclassified Information (CUI)" under the clause.

For Charles River, the development of this standard certainly represents a critical step forward in combatting the cyber threat. However, it has also missed the mark in several critical ways. The NIST standard targets the protection of CUI. But, what is CUI? It obviously includes U.S. federal government information that is considered sensitive, but not classified. But, one of the "selling points" of NIST compliance is that it also targets the protection of the proprietary and confidential data of our company, the PII of our staff and our customers. But, until we can confidently identify and label CUI, we are challenged in its protection.

The Deputy CIO of the DOD, at one industry meeting attended by our IT team in 2017, responded to a question about the department's challenge in properly defining and marking CUI sent to our facility, by saying "we are working on that, but we don't have a plan in place right

now." To this day, CUI sent to our facility by DOD customers is often improperly identified and marked—and we know it. This has been a critical concern in our decision-making around NIST compliance implementation. Because CUI data is not always clearly identified, we chose not to put our staff in the untenable position of making those calls on the fly in their daily work. So, we declared that all data on our corporate networks is to be treated as CUI for compliance purposes. Therefore, all network devices had to be equally compliant with the standard. This may sound simple … it has been far from it.

Given the lack of clarity in how we were to approach the NIST standard, I am very proud that our IT and Software Engineering teams, recognizing the importance of the goal of better protecting our company's and the government's data, took on the challenge with gusto.

However, they encountered multiple non-fiscal issues with ensuring compliance. First, NIST implementation requirements are vague. All of the 110 NIST controls can be approached and implemented in a variety of ways, and there is a dearth of *specific* guidance, information, or documentation on preferred implementation methods. As a result, we spent approximately 800 person-hours between April and July of 2017 on research and discussions with external consultants to interpret the control requirements. Second, the NIST document was written in a manner and voice unfamiliar to us, even though we have been working with the DOD and other federal agencies for more than 35 years. Finally, we found that many of our customers, from contracting officers to technical sponsors to senior staff at the Pentagon, seemed equally confused and unable to provide helpful clarification and guidance.

Fortunately, being a software engineering company, our team is very technically savvy and highly experienced. After deciphering all of the NIST controls, we were able to develop a Risk Gap Analysis and formulate a plan of action. We then spent an additional 1,500 person-hours between August and December of 2017 to implement that plan. It was a significant challenge to meet all of the requirements with the limited amount of information and guidance provided. Furthermore, while we are confident that Charles River Analytics is fully NIST-compliant, we are still not sure how or when that compliance will be confirmed through audit.

The costs of NIST compliance were quite burdensome as well. Charles River Analytics ended up spending more than $300K in hardware, software, vendor maintenance contracts, and license tier upgrades. While allowable and allocable to our government contracts, these costs were entirely unbudgeted, and adversely affected the cost mix on our projects for fiscal years 2017 and 2018.

The unexpected costs did not end with these one-time-only purchases—Charles River Analytics now estimates that we will spend an additional 30 percent every year on non-labor IT overhead, for as long as the company continues to sign contracts containing the updated DFARS clause requiring NIST compliance. Now, I recognize that as a software engineering company operating across a number of sites, our IT infrastructure may be significantly more complex than the average U.S. small business, and so, our costs may be on the higher end of the spectrum.

However, we cannot kid ourselves that true NIST compliance can currently be achieved at a minimal cost to businesses.

The labor costs associated with ensuring NIST compliance were diverse and varied, and high across the board. Apart from the cost to interpret, discuss, plan, and implement compliance solutions, NIST compliance has required additional and ongoing costs that have affected previously planned initiatives, backlogged other infrastructure upgrades, and future quality-of-life improvements (which indirectly affect staff retention issues). Planned and ongoing infrastructural maintenance/improvements were either delayed, resulting in an increased overall cost of roughly 20 percent across the board, or were "solved" by spending money on external consultants, at an approximate markup of 200 percent over qualified in-house labor. By mid-2018, the IT Department staff (and therefore, our overhead IT costs) was increased from five to eight full-time staff, specifically to support our ongoing infrastructure work and maintain NIST compliance.

Finally, NIST compliance, as currently defined, places a significant burden on our technical staff and on our frequent partners. Creating and maintaining compliant infrastructure drains resources from project work, resulting in less progress per dollar, and makes it more difficult to put contracts in place with other research organizations, including universities and other small businesses. NIST assumes that the software configuration of a workstation will remain relatively static and contain well-known software, which is simply not the case for an R&D-driven software engineering company, such as Charles River. The resulting controls add significant resource and time barriers to the execution of R&D, as a key ingredient in such work is exploring and analyzing multiple solutions, each of which must be made compliant. This effectively raises the overhead of compliance in areas that we cannot afford—that is, finding solutions for the coming years and decades.

Small businesses must also analyze commonly used tools (e.g., inter-organizational collaboration tools) for NIST compliance, further impairing collaboration and productivity. Perhaps most importantly, NIST compliance hinders and frustrates top-performing personnel, causing them to seek employment in other sectors, making it difficult to maintain competitive business advantage and competitive national advantage. Ultimately, NIST significantly impairs a small business's ability to do defense-driven R&D, and to be forward-looking, effectively handing advantages to our nation's adversaries.

Charles River Recommendations

Given the challenge, expense, and business impacts of Charles River's NIST compliance program, I recommend improvements to the government's specification and support for its implementation by small defense contracting businesses across three areas.

First, we require *clarity* in the definition and management of Confidential Unclassified Information (CUI), both provided by our DOD customer base, but also information generated by our company in the course of business execution. Second, we require *flexibility* in the application of the defined NIST controls. IT requirements across industries and companies varies widely, and the implementation of NIST-compliant controls should reflect this diversity in IT system needs. Finally, we require *clear guidance* to support the nation's small businesses in the defense sector to comply properly. This guidance must be delivered in easily accessible implementation guides—using plain language—that target the range of IT challenges faced across the community.

If programs like the NIST SP 800-171 are to be leveraged outside the government contracting sector, it will also be imperative to incentivize large IT commercial vendors, such as Microsoft, Amazon, and Cisco, to develop NIST-compliant variants of market-leading IT products. Then, and only then, can this valiant effort begun by the NIST SP 800-171 standard be extended to the U.S. small business community, in its entirety.

Conclusion

Federal government agencies rely upon external contractors to carry out a wide range of functions. Many contractors have access to sensitive data that could, if compromised, potentially reveal classified information, threaten national security or even put lives at risk. As a result, cybersecurity is a critical and growing concern for both federal agencies and those who do business with them.

However, the implementation requirements for NIST SP 800-171 is just one example of the barriers small businesses face when engaging in the federal acquisition process. As demonstrated throughout my testimony, not only is the cost of compliance significant, the required overhead is quite extensive, costly and onerous on both prime contractors and subcontractors who need to be compliant.

Understandably, many small businesses feel overwhelmed. If you don't comply, your contracts – and, perhaps, your business – are at risk. Yet, many do not know where to begin or even after all their efforts, know if they are truly compliant. Unlike Charles River, many small businesses do not employ a dedicated IT employee or consultant. Often, an owner or key employee performs IT functions in addition to their regular duties. And even Fortune 500 companies with vast resources struggle with information security. No wonder small-business owners feel overwhelmed when dealing with cyber protections!

Still, when you submit a Request for Proposal (RFP) or sign a contract containing one or more information security clauses, you are affirming your ability to comply with the contract. You need to employ as many best practices as possible to show that you have employed good faith due diligence to achieve compliance. As with any compliance program, you must be able to

demonstrate that you are doing – or trying to do – the right thing. Nonetheless, the NIST SP 800-171 requirement makes this extremely hard to do. Therefore, it is critically important for Congress to always bear in mind the unique challenges that small businesses face when it comes to cybersecurity and continue to include the small-business community in the process of preventing unnecessary burdens that could accompany efforts to stem cyber-attacks.

Thank you for allowing me to testify before the committee today. I would be happy to answer any questions you might have for me.

Chairman RUBIO. Thank you.

I'm going to defer my question time to Senator Hawley, who I think has to go and do something right away.

Senator HAWLEY. Thank you very much, Mr. Chairman. Thank you, Ranking Member, and thank you to the witnesses for being here.

Ms. Harper, I just want to stay with you. The citizens of Missouri, my home State, have been faced with a series of cyberattacks across a range of industries.

Last year, Blue Springs, which is in the Greater Kansas Area, the Blue Springs Family Care was hacked by malware and ransomware, and nearly 45,000 patient records were stolen, including patients' Social Security numbers, account numbers, driver's licenses, medical information, and so on.

We had another case in Fort Leonard Wood, which I think the Chairman mentioned earlier, in which Fort Leonard Wood, our military installation there removed surveillance cameras made by Chinese manufacturers due to significant security concerns.

As I just listened to your testimony, as I read your written testimony and those of your fellow panelists, I was struck by the sheer magnitude of the problem, but also what you have just been talking about, the incredible difficulty of complying with the NIST standards.

You suggested something I found interesting, which was in your written testimony, which was incentivizing large IT commercial vendors to develop NIST-compliant variance of market-leading IT products. Can you just say something more about that idea?

Ms. HARPER. Absolutely.

We all agree that the threat is paramount. It is a targeted threat in many cases. It is a challenging threat for the entire Nation, for all of our institutions, our companies, small businesses, and us as individuals. We cannot minimize the threat, but the way that we address that threat is still very nascent in my opinion.

As we have gone through our NIST compliance program, which took an immense amount of effort and challenge for a very savvy, high-tech software engineering company, small businesses in this country that do not do the work we kind of do, do not stand a chance to be as effectively implementing something like NIST 800–171, at least.

So can we transfer some of the requirement for that on to the IT sources that we all already rely upon? So Office 365 for Microsoft and AWS with their Web service and cloud infrastructure. Is there a way that the Government can incentivize those players in the industry as well as the hardware side with Cisco, et cetera, to augment and provide NIST-compliant versions that will take the complexity of this process out of the game for small businesses that do not have the technical savvy that my staff does?

Senator HAWLEY. Is it your thought or hope that this would make these sort of protections, effective cybersecurity, more affordable for small business as well? I mean more widely available, more affordable, easier to implement.

Ms. HARPER. Many of us already pay a great deal of money to manage our software licenses for these very common tools. Aug-

menting that cost to get a NIST-compliant collection at a reasonable cost seems a very reasonable approach.

If my IT staff could have bought AWS NIST-dot-1, dot-2, we absolutely would have done it, and we probably would have spent a lot less than $300,000 in doing it.

Senator HAWLEY. Yeah. The costs that you outlined in your testimony here are just extraordinary.

What can we do? What might this Committee do to help make this happen?

Ms. HARPER. So, first of all, I think recognizing the NIST Standard 800–171 is a really valiant attempt to address this set of threats that is facing us.

I do not want it to go away. I want it to be a more manageable process. I want it to be more accessible, even to a staff like mine.

When we were introduced to the requirements for NIST—and I will say this anecdotally at best—my IT team pulled me and my CFO into a conference room and spoke to us for about 2 and-a-half hours, and we left the room feeling quite ill. We could see exactly the cost that was coming at us, but the cultural impact that this has also had on our company.

So I do not want to dismiss any of the value of NIST. I want to recognize that where we are right now is not good enough in supporting its implementation. I would like to see Congress able to support NIST and other organizations like SBA to provide access to recipe guidelines for various companies that have IT requirements—X, Y, and Z. Here are the five things you need to buy and implement. If you need to do lots of other things in A, B, and C, then here is the extra complexity—more complex set of things that need to be done.

That level of documentation, spending, 4 of our 8 months of implementation, just trying to interpret the controls was disconcerting, at best.

Senator HAWLEY. That is extraordinary.

Yeah. Thank you so much for your testimony. Thank you for being here.

Thank you, Mr. Chairman.

Chairman RUBIO. Ranking Member.

Senator CARDIN. Well, I thank all of you for your testimony.

Ms. Harper, I am trying to get a handle on exactly how we can accomplish the objective that is critically important when you are dealing with Federal agencies that have sensitive information, and we expect the contractors to have security for that information, how we achieve those objectives, but do it in a way that is less burdensome and certainly less impact on the work of your talented people.

We appreciate the follow-up for today. You certainly have piqued our interest, and we are still a little bit confused as to how we should proceed in order to deal with some of the issues that you have raised. So I hope you will feel comfortable in working with us to try to figure out how we can accomplish this.

Ms. HARPER. I and my staff would be more than happy to help to shape some activities.

I think that it will be important to recognize different requirements and recognize the different companies.

Yes, we are a defense contractor. We hold a great deal of sensitive information that is not classified, and we recognize the importance of that.

We equally recognize the importance of our own data and our staff data.

So protecting all of it is imperative, but there has to be a more flexible way to go about implementing this kind of standard than we have accomplished.

Senator CARDIN. And I appreciate it. I appreciate that attitude, recognizing we need to do it.

Ms. HARPER. Yes, absolutely.

Senator CARDIN. So let us figure out the best way to do it.

Ms. Hyman, I looked at some of your numbers, and I am thinking that there are a lot of small businesses that have been compromised that do not come forward and tell us. Either they are embarrassed or they do not want their customers to know they have been infiltrated. So we do not even have the full numbers of small businesses that have been compromised through cyberattacks.

What have you found is the best selling point to get a small businesses owner focused in the right direction as to how to deal with their cybersecurity needs?

Ms. HYMAN. Senator, thanks for the question.

To your point, one thing that I would present to you is that we have a very robust research department at CompTIA, and we are open to and would welcome the opportunity to do more research into the small business situation, try to get to the bottom of what some of the challenges are that they are facing in addition to what we have put in our written testimony.

But we work day-to-day with a lot of small businesses and particularly on the managed service side of things. We have an IT security community which is sort of a crowdsource group of companies, and so we are able to talk to them about the dollar value, what is their exposure from a business point of view. And it is really the title of this hearing. It is an existential threat, and they could ultimately go out of business if they are not paying attention to some of the basic issues that are out there.

The other thing is because we are a certifying body for the workforce, we are very focused on trying to attract talent and make sure that that one person in that small business has the requisite knowledge and can validate their skill sets, so that they can at least have an opportunity to manage what they need to manage on a day-to-day basis, but also have the education and expertise to work with managed service providers, managed security providers. That third-party relationship is really vital I think to a lot of small businesses, particularly not those that are in software, but like an HVAC company.

Senator CARDIN. Certainly.

Ms. HYMAN. Yeah.

Senator CARDIN. Thank you. That is very helpful.

Ms. HYMAN. Yeah.

Senator CARDIN. Of course, I am very proud of what Maryland has done. Ms. Smith, congratulations on getting that legislation through the Maryland General Assembly because obviously cost is an issue. There is not a lot of flexible funding for a company that

has one employee. So for them to get the expertise they need to deal with cyber, it is a challenge financially.

So the credit in Maryland seems like a very attractive tool. I think I heard you say somewhere around $4 million in credits for——

Ms. SMITH. Yes, sir. Yes. That is the year 2019. There is $4 million available for tax credits for that program.

Senator CARDIN. So it is a little early, I guess, to know the exact impact here, but can you just tell us what you have been hearing from the small business community in regards to the attractiveness of this tool and getting the focus on cybersecurity?

Ms. SMITH. Sure.

I hear more on the side of our cyber companies telling us, "How do I apply? How do I get approved as a seller?" But we work closely with the Better Business Bureau of Greater Maryland and Regional Manufacturing Institute, as I mentioned, and they are getting the word out to their businesses who are excited about it, trying to figure out how do they access it.

I think because it is so new, just in October, we got the final details all worked out and are able to release it.

But working even with the MEP group organization in our State, we have done some programming to let the businesses know about it, and they are very excited that it is there. It is just right now figuring out who is the qualified sellers that they can purchase those products from and what do they need. A lot of them do not even know what do I need, where do I start. So just connecting them with the right resources, that is where we are playing a role in helping them identify those.

Senator CARDIN. I am a believer in federalism. So we are watching very closely what you are doing in Maryland. We might try to take some of those programs and look at them as national programs. So we will be following very closely what is happening in the great State of Maryland. So thank you very much.

Chairman RUBIO. Senator Kennedy.

Senator KENNEDY. Thank you, Mr. Chairman, and I want to thank our witnesses for being here today.

I mean, most small businesswomen and businessmen are busy earning a living and trying to make payroll. They read about the need to enhance their cybersecurity, but most of them—and many Senators—do not know where to start.

Tell me again what Maryland has done to try to educate small business people.

Ms. SMITH. Well, our organization is primarily focused on our cybersecurity companies growing and generating sales. So we have partnered with a lot of business organizations in the State that do help the small business community or even larger businesses to access whatever they need to be cybersecure.

So we create programs throughout the year. We have a big event coming up in April where they can connect face-to-face. It is called our Maryland Cyber Day Marketplace. We will have about 100 of our cyber companies there. This year, we have created what we call "Information Station," so they can come and, if you do not know where to start, somebody will guide you. So just partnering, I

think, with those organizations, other organizations, and also having an online directory. Most States do not.

Senator KENNEDY. Tell me what, if anything, does the SBA do here. I mean, if I am a small businessman and I want to enhance my cybersecurity and I call SBA and say, "How do I enhance my cybersecurity?" What are they going to tell me?

Any of you.

Ms. SMITH. I know that we see SBA members or staff people at some of the events that we go to, so I know they are out there.

I was not aware that the SBA had cybersecurity resources until I was asked to testify here, so I do not know.

Senator KENNEDY. What would you advise me as a small businessman? I come to you and I say, "I want to enhance my cybersecurity. Where do I go? What do I do?"

Ms. HYMAN. I would say there are a number of different avenues, but I think one of the—well, I mean, there is the National Cybersecurity Alliance. There are the SBDCs, which are starting to try to take a more vocal——

Senator KENNEDY. What is an SBDC?

Ms. HYMAN. The Small Business——

Ms. HARPER. Development Center.

Ms. HYMAN [continuing]. Development Center. Thank you.

So they are localized. For example, I was looking at the Michigan SBDC earlier today, and they have developed a very comprehensive website, which is great. It is a start.

But we also work with NIST, for example, in terms of what they do, or DHS has local—localized efforts to reach out to small businesses. But I will tell you it is a very dispersed conversation.

So, as a nonprofit trade association, we are constantly trying to educate our membership, and it ranges from managed service providers to small companies to large companies, but we are trying to educate them as to the resources that are out there. That is a role that we can play, partnering with these various public entities.

Senator KENNEDY. Ms. Harper, do you want to add anything?

Ms. HARPER. Senator, I believe that being a small business owner and not having the technical background that my company does—and you recognize that there is this threat out there that you do not understand; you do not understand how it impacts your systems, your payroll systems, anything else that you are housing in your organization—sadly, I would say I bet people start with google.com and start looking for some resources.

I would hope that the presence of SBA and the NIST Cybersecurity Framework and things would pop out as resources to that small business owner to provide that, but I am quite confident that they do not know about it today.

Senator KENNEDY. Okay. You may or may not know this, but I assume most small business people start thinking about cybersecurity after they have had a problem.

Would that be——

Ms. HARPER. As a research company very focused in cybersecurity, I would like to think we are a little ahead of the game, but understood.

Senator KENNEDY. With the exception of your company.

How do we reverse that? I try to put myself in the shoes of the small businessperson. Again, you are working hard. You are trying to make payroll. You read these articles about cybersecurity, but you do not know where to start.

Ms. HARPER. And furthermore, sir, when you see the news and you recognize that TJ Maxx and OPM are being compromised, how do you even hope to start——

Senator KENNEDY. That is a great point. That is a great point.

Ms. HARPER [continuing]. And provide that? So you are hoping that industry is going to rally around you and provide you, hopefully, with the tools that are being developed to protect those kinds of industries, and hopefully, you can afford them once they are available.

Ms. HYMAN. I wonder also if there is a message to be delivered, which is that it is a competitive advantage for a small business to have taken on certain steps that show they are aware of cybersecurity and that they need to differentiate themselves from the guy down the street. That is certainly one thing to talk about.

But you are right. This is a very comprehensive effort required from an educational point of view, from providing reasonably affordable tools that are out there, and making that business case.

Ms. SMITH. As I indicated in my testimony, one of the reasons that companies say they do not implement cybersecurity programs or invest in cybersecurity is they do not know who to use. That Google search is going to turn up a ton of resources, so maybe having resource directories of cyber providers.

Senator KENNEDY. That is just going to give you Google's preferred providers.

Ms. SMITH. Right, right. Who pays Google, right, would be at the top of the list.

Ms. HARPER. And, by the way, the phishing folks on the other side using that as a capture.

Senator KENNEDY. That is a good point.

Thank you, all three of you. It was very interesting, very helpful.

Chairman RUBIO. Senator Duckworth.

Senator DUCKWORTH. Thank you, Mr. Chairman.

Ms. Hyman, we all know that cybersecurity has become more important than ever for businesses of all size, and I wanted to sort of follow on the thread of the discussion so far.

Say you have an entrepreneur coming to you. Can you explain why entrepreneurs in businesses of all size, including the smallest startups, should be thinking about cybersecurity and how it plays an essential role in protecting their customers? As you said, it is a competitive advantage. So you have someone who is starting a company. They are just getting started, and they come to you. How do you talk them through this? How do you talk them into making the investment in cybersecurity, when they are just trying to get this thing set up? And how do you explain what the steps should be as they go through this process?

Ms. HYMAN. It is a great question. Thank you, Senator.

I think what I would like to do is just take one step back and share with you a little bit of research that we have done recently at CompTIA with small businesses that was not directly related to cybersecurity, but had some interesting results.

So the five technology areas of concern among SMBs, the top five, number one was figuring out how to integrate different applications, data sources, platforms, devices, number one. Number two, effectively managing and using data, because any company now is trying to figure out how to make that customer experience a better one. Number three, cybersecurity and data cybersecurity. Number four, modernizing aging equipment or software; and number five, getting more ROI or a bang for the buck, if you will, from technology investments.

The reason I raise that with you is those are the top-line concerns for 650 SMBs that we actually surveyed, and I think that is representative of a lot of companies around the country. So what are they asking for? They are asking for tools to be able to figure out how to do all these things.

One of the proposals, I believe, in the legislation is to have an SBDC official who might be able to provide assistance and guidance on some of these things. We would recommend that that individual be certified with an industry-recognized credential so that they have the wherewithal to help answer some of these questions. That is the beginning of a conversation.

I would also say in terms of what resources are needed, training for the companies themselves. I mentioned earlier that oftentimes in a small company, there might be one person that is sort of responsible for taking care of the computers. Well, if that person had, for example, the investment in some sort of training—for us, it might be IT fundamentals, which gives a basic overview of what the technology landscape looks like and starts to get into some basic security issues or even an A-plus exam, and there are other groups like ours that do this. But if they have that initial training opportunity and the investment for that, they can do some of the basic things that they need to do, and they can also interact well with third parties.

One thing I want to point out that I think is very interesting is on the updating and modernizing of equipment. So I understand a startup may well have newer issues, but pretty soon, they are going to have some of those problems as well.

I do not know if you have looked at your Microsoft 7 and said, "Oh my God, I cannot even get service for it anymore." So how do we continuously upgrade and modernize technology? I think that is an important investment to be made.

So I hope that answers your question.

Senator DUCKWORTH. It does.

Is there any move towards a certification program or something where either the businesses can be certified if they are handling a lot of data as, hey, we have gotten this Good Housekeeping Seal of Approval, good cybersecurity is installed, that becomes an advantage that they have over their competitors?

Then also, on the other side of that, as they are looking for people who are experts, they go to the Google search. How do they know which companies are legit and which ones are really going to provide them with the right advice to move forward?

Ms. HYMAN. Well, I will share that CompTIA had a Trustmark program in place, and the IT Security Trustmark is an organizational credential. It is totally voluntary.

When we first unveiled it, it was mapped to the NIST Framework. We found even thought we had pared that down rather significantly, it was still a big challenge for small businesses to meet a lot of the requirements of that Trustmark.

But one of the things that we raised in our written submission was that perhaps that is something, working with companies like Charles River and elsewhere, where we can start to really define and pare down more significantly what that organizational credential looks like.

We are happy to volunteer and give our organizational credential so that there is at least a basis for that conversation, and you can look at it. And then we can figure out how do we make that even a more effective credential going forward.

Senator DUCKWORTH. Thank you.

Ms. Harper or either of one of you, do you want to add something to that?

Ms. SMITH. One of the things I wanted to mention is we have talked with our local Better Business Bureau about doing something like that, but looking at us as a small nonprofit saying where do we start with this, it was too much of an uphill climb for us. But the BBBs are there to ensure as a consumer, who are you buying from, who do you trust, and maybe that is an organization that would be good to involve if something like that would happen.

And we have talked about it even in the procurement process for the State if a business was certified, whatever that is, that they might get a preferential treatment in the procurement process with our local State government.

Senator DUCKWORTH. Thank you.

Thank you, Mr. Chairman.

Senator CARDIN. Mr. Chairman, just for one observation, if I might, because Senator Kennedy raised a very good point about the capacity of the SBA.

The SBDCs are clearly an entity that could help on cyber. The letter that we wrote, this Committee, to SBA urged them to look at the SBDC's capacity to deal with cyber-trained helpers. I just mention that.

Then Ms. Roat's testimony was they have limited resources in order to deal with it.

Just one observation, if I might, since this is the week the President's skinny budget came out. He happens to cut—the Trump budget cuts the SBDCs by 23 percent. I know that we will do things here that will be different than the President's budget. I understand that, but I do think we also have to be realistic about the resources that are made available to the SBA.

Chairman RUBIO. Thank you.

I just have one. I mean, my colleagues have covered a lot of the topics that I wanted to ask, but there is one. I think you have touched on it just a little bit.

But I am curious about CAMI and its role in representing so many small businesses that are afraid to come forward and discuss vulnerabilities. Obviously, it has business impacts. On the one hand, obviously, if there is a breach of some sort, you want people to know about it; on the other hand, many businesses that are

small and midsized businesses would struggle with a public disclosure that could theoretically, reputationally wipe them out.

So how is CAMI handling that? What is it doing? First, it sort of highlights the number and severity of the attacks that are on small business, and then, in particular, helping small businesses that are afraid to come forward and discuss their vulnerabilities because, frankly, from those attacks is how we can improve our method of responding and preventing them.

Ms. SMITH. Sure. One of the things that we are implementing—and it will come out in our revised website in April—is case studies, which allows our members to talk about businesses that have been breached and what they did to remedy the situation and the cost involved and the steps that they took and things that they might have been able to do ahead of time to prevent that.

So I think illustrating it through this is a manufacturer, this was a small retail organization, so they can say "okay, that is me," just to know that someone else has gone through it.

And contacting us, one of the things we do is anonymously put out a plea to our members. If anybody is available to handle this situation, so the business is not—their contact information or name is not out there, to then connect them with resources and give those resources to the business that is looking for that. They can also directly contact the businesses through our website.

But that fear factor is certainly there, but that is also after they have been breached. If we can get to them before they have been breached and say, "Put these protections in place," many of them would not suffer those breaches or attacks.

Chairman RUBIO. But the existence of those case studies, without outing a company, is very helpful to a small company that sees themself reflected in the case study——

Ms. SMITH. Absolutely.

Chairman RUBIO [continuing]. And understands that someone like them could also be hit by this.

Ms. SMITH. Absolutely.

One of the things that we find all the time in what we do, even our organization when we were first created, we expected businesses to come to our programs and hear a talk on cybersecurity and how to be cybersecure. They do not do that.

Our local SBA rep said the same thing, that they have tried to do programs for the small businesses, and they do not come. They know they have got to be secure. They are too busy or it does not apply to them, whatever.

But going to organizations that are already doing things and making it a piece of their conference, put the information on their website in addition to the SBA website, things like that, small things that can be done, taking the message out to the business and marketing.

We deal with our local government. They do not want to spend money on marketing and getting the word out, but you have got these great programs. How do you get the word out? And there has got to be some kind of method for telling the message and promoting what resources are available to those.

Chairman RUBIO. Well, I want to thank all three of you for being patient and being with us today. We have had a great hearing, and

your input, as you saw from the questions and comments of some of our members I think has elicited thinking about, number one, things people may want to take back to their own States, but more holistically some of the challenges we face as we move forward on what SBA can do and what the Federal Government can do to empower small businesses to confront this very real 21st century challenge, and again, we thank you for being willing to be a part of this today because it is very helpful to us.

The hearing on the record will remain open for 2 weeks, and any statements or questions for the record should be submitted by Wednesday, March 27th, at 5:00 p.m. and again, thank you so much for being here, and with that, this hearing is adjourned.

[Whereupon, at 4:11 p.m., the Committee was adjourned.]

APPENDIX MATERIAL SUBMITTED

Senate Committee on Small Business and Entrepreneurship Hearing
March 13, 2019
Follow-Up Questions for the Record
Maria Roat – SBA CIO

Questions for Ms. Maria Roat

Questions from:

Chairman Rubio

In recent years, foreign state-backed firms have successfully breached U.S.-based security systems, obtained confidential information, and interfered with democratic systems. Since the majority of American businesses are categorized as small, this means that small business IT systems are a large part of American infrastructure that needs to be protected against cyber criminals.

QUESTION 1:

What is the federal government doing to make small businesses aware of the threat of cyber-crime and to prepare them against cyber-attacks?

The U.S. Small Business Administration (SBA) provides counseling and training to entrepreneurs and small business owners on cybersecurity through the Small Business Development Centers (SBDC) program. The SBA also provides a free online training course through the SBA Learning Center on the ways small businesses can protect themselves from a cyber-attack, available at www.sba.gov/learning-center. The SBA also has a partnership with the Federal Trade Commission (FTC) to provide information on cybersecurity to small business owners through the FTC website.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) leads the federal government's efforts to safeguard and secure federal civilian and private sector networks from cyber risks. CISA works with the Small Business Administration, to engage America's small businesses. CISA makes available to small businesses cybersecurity threat information, guidance on best practices, and a full range of technical assistance. These resources can be found online at: https://www.us-cert.gov/.

QUESTION 2:

How can Congress better assist you in these efforts?

SBA appreciates the interest and support of the committee and will continue working with you as SBA identifies areas for potential coordination.

There is now ample evidence that Chinese companies have used their technical products to spy on and interfere with American activities. Last February, FBI Director Christopher Wray testified to the Senate Intelligence Committee that smartphones made by Chinese government-owned companies, like ZTE and Huawei, have the "capacity to maliciously modify or steal information." The 2019 National Defense Authorization Act restricted federal government use of products manufactured by Chinese-based technology firms for "substantial or critical components of any system," or as "critical technology."

QUESTION 3:

What is the federal government doing to ensure that it is not using these Chinese products?

The Department of Homeland Security (DHS) is leading federal efforts to address the complex challenges involved in managing risks associated with global, interconnected supply chains. Their recently announced Information and Communications Technology (ICT) Supply Chain Task Force establishes a valuable partnership across industry and among key federal agencies to examine and develop recommendations to identify and manage risk to the global ICT supply chain. The committee can learn more on the initiative at: https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members

QUESTION 4:

Have you examined the SBA's systems to ensure that there are no Chinese-manufactured products?

The SBA has been examining our systems and is working to fully implement the requirements in Section 889 of the 2019 National Defense Authorization Act, which placed prohibitions on the procurement or contracting of certain equipment, system, or service that uses covered telecommunications. As part of my overall modernization strategy, I have implemented next generation cloud services that leverage artificial intelligence and machine learning to streamline agency-wide monitoring and detection of anomalous activities. Using these tools, my team can maintain situational awareness of telecommunications and video surveillance services and equipment across the SBA environment.

Many small businesses are unaware of the impending threats they face from cyber-attacks. Others are aware but confused by the abundance of varying government resources available to them. Small businesses will currently find information that is presented as authoritative, current, and designed specifically for them on the websites for the SBA, FTC, FCC, NIST, DHS, and others.

QUESTION 5:

How can agencies work together to ensure that small businesses are getting up-to-date and accurate cybersecurity information?

The continuous focus and prioritization of cybersecurity across all sectors has helped raise awareness and led to the development of numerous resources and best practices for small businesses. Federal agencies need to continue these efforts and ensure the information remains relevant and accurate, and that any gaps are identified.

QUESTION 6:

Should all of these sources point back to one authoritative resource?

Numerous resources, especially those produced by DHS's CISA and NIST, may serve as authoritative sources. I believe relevance and accuracy are most important when it comes to these resources.

QUESTION 7:

Is the SBA relying on the NIST voluntary guidelines for small business owners in developing its trainings and materials?

Under the leadership of Administrator McMahon and Secretary Nielsen, the Department of Homeland Security and the U.S. Small Business Administration collaborated with America's SBDC's to provide a report on the resources available to small business owners on cybersecurity.

The IT systems at the SBA were in dire conditions prior to your arrival there just over two years ago. You have mentioned in your testimony that the SBA has made great strides in modernizing its IT equipment and in updating systems. This has been confirmed by the House Oversight and Government Reform Committee's Biannual IT Scorecard, which reported that you received a "B+" rating, the highest that any agency received. However, you also received some troubling ratings, including a "D" in transparency and risk management, as well as an "F" in cyber.

QUESTION 8:

Do you know why the SBA received such low grades in categories that seem very important such as risk management and cyber?

We appreciate that this committee is very aware of the technology challenges faced by SBA and the inconsistent leadership over the past decade. Numerous audits and published reports have clearly established the need to modernize IT and establish an enterprise program across the agency. The success with fully implementing the Federal Information Technology Acquisition

Reform Act (FITARA) has also led to a greatly improved cybersecurity program. The key element being the establishment of enterprise IT and cybersecurity services. Working across the agency with every program office, I was able to fully deploy key cybersecurity services that have already improved the agency's risk management scores. Specifically, the agency is meeting 6 out of 10 cross agency priority (CAP) goals in FY19. This is the first time the agency has met this mark. We also have now established a FY18-22 Cybersecurity and Privacy Strategy, of which the enterprise security services is a component.

SBA received a low grade in the risk and transparency section as a result of how GAO calculates the risk and transparency score, based on the number of major investments with a risk rating of yellow or red by dollar amount. The total major investment portfolio is divided by the total number of investments rated yellow or red, which calculates the Agency Risk and Transparency percentage. That percent is then compared with other agencies, and the top five agencies with most reported risks by dollar are given an A, the next five B, etc. SBA's major investments totaled $43M, and $13M, were rated yellow which equaled a score of 31% (D) as compared with other agencies.

QUESTION 9:

What are your plans to make improvements in these low-graded categories?

To improve the risk and transparency score, SBA has added more rigor to the risk management process by rating all our modernization programs yellow due to the complexity of the modernization efforts. This has increased the total number of major investments that are rated yellow from 31% to 80%, which should increase SBA's overall grade as compared to other agencies.

QUESTION 10:

Can you update us on your progress with complying with the IG and GAO's recommendations?

When I arrived in October 2016, the agency had approximately 50 open OIG recommendations addressed to the CIO, many longstanding and delayed. I established rigorous management and focus of all audit findings and the current number of open OIG recommendations now stands at 5. These 5 remaining findings are the most complex issues involving legacy and sometimes critical systems that we are working to modernize over the next 2 years.

There are 12 GAO audits in progress, and 8 closed audits with 10 open recommendations. We are working closely with GAO to close the 3 oldest findings this fiscal year.

QUESTION 11:

What next steps do you have planned?

Under my direction, the Office of the Chief Information Officer continues to move aggressively to address deficiencies and to improve SBA's cybersecurity posture, governance, and oversight,

and to stabilize and modernize SBA's networks, systems, data centers, and overall operations. As a result, long-standing GAO and OIG audit findings are either closed or nearing closure and we will continue to work with audit personnel to effectively address findings as they are identified.

QUESTION 12:

How can this Committee help you strengthen the SBA's IT security?

SBA appreciates the attention and support of the committee. With the resources provided, I have built a strong cybersecurity foundation that I believe serves the needs of the agency. Going forward, my focus involves eliminating legacy IT systems and technologies. I will continue to build modern, enterprise services that enable the business of the agency and provide the strong security posture required to protect entrepreneurs. I will continue to remove silos and drive standardization and cyber hygiene. I only ask for your continued support as I work through the complex challenges to achieve the best technology position to serve the nation's small businesses.

The SBA has made significant improvements to its website and we understand that you are working to make training materials available online. Unfortunately, numerous constituents in Florida voiced that the process for applying for, and receiving disaster loans, is slow and outdated, requiring them to go into disaster service centers to fill out mounds of paperwork.

QUESTION 13:

Have you considered ways to improve SBA's service to disaster victims through more modern technology?

To enhance the agency's disaster response staffing efforts, SBA has added virtual desktop and other cloud capabilities to improve our surge staffing capacity and to better enable our disaster employees to work remotely. Also, our Office of Disaster Assistance (ODA) has greatly improved the loan process through technology, reducing the cycle times for loan application. SBA made significant strides over the past two years with improving and modernizing its disaster loan origination system. SBA's aging Disaster Credit Management System (DCMS) was redesigned and re-platformed on state-of-the-art cloud technologies, to aid with high volume loan processing and to establish a long-term foundation for enabling secure, flexible and rapid responses to changing conditions. The key goal of the DCMS modernization effort is to improve SBA's ability to serve the disaster survivor through:

- Streamlining and/or eliminating institutional processes that were cumbersome or did not provide value;
- Maximizing the impacts of modern technology on ODA business processes;
- Supporting volume processing functions such as exception processing, parallel processing, and improved workload management.

QUESTION 14:

Are you considering a mobile platform for disaster loan application and tracking?

SBA's Disaster Loan Assistance Portal (DLAP), the public facing web portal for submitting disaster loan applications, has undergone several improvements over the past two years to optimize the website for mobile purposes. Those improvements include:

- Introducing dynamic layouts which adapt to different screen sizes for mobile devices;
- Eliminating browser 'pop-ups' to allow for better experiences on mobile devices;
- Adopting HTML 5 / CSS standards for increased control over presentation and layout.

SBA is considering additional enhancements to make the DLAP as accessible as possible to all end-users.

The Global Cyber Alliance (GCA) is a non-governmental organization that works between sectors in an effort dedicated to eradicating cyber risk and improving internet exchanges. GCA offers a free checklist with free tools, software, and services for small businesses. NIST has opted to make this checklist available on its webpage.

QUESTION 15:

Have you previously engaged with GCA on any initiative?

OCIO has not, to my knowledge, engaged with GCA.

QUESTION 16:

Would you be willing to provide GCA's checklist on your webpage an effort to make these services available to small businesses?

We appreciate the recommendation and will review and assess the information they provide.

Senate Committee on Small Business and Entrepreneurship Hearing
March 13, 2019
Follow-Up Questions for the Record

Questions for Dr. Charles Romine

Questions from: Chairman Rubio

The Committee heard from small business contractors at the March 13th hearing that the cost and time required to comply with the NIST 800-171 special publication are extremely onerous. Even sophisticated businesses that specialize in cybersecurity services told the Committee that they needed teams of consultants, thousands of hours, and hundreds of thousands of dollars to even initially come into compliance with the requirements from this publication. Yet, if companies cannot prove compliance with this publication, they are unlikely to win federal contracts.

The burden of SP 800-171 has been a long-standing problem for small businesses. On February 29, 2016, the Office of Advocacy at the SBA sent a letter to the Department of Defense, urging the DoD to consider alternatives to its interim final rule "Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services." Advocacy pointed out that the DoD had not considered the significant impact of NIST SP 800-171 on small prime and subcontractors when it estimated the economic impact of compliance. Last November, Advocacy again highlighted the burden of compliance with SP 800-171 for small businesses with its comments on the draft initial regulatory flexibility analysis for FAR2017-016 on controlled unclassified information (CUI).

QUESTION 1:

Did NIST intend for the FAR, DoD, DHS, and other agencies to adopt the ideas of special publication 800-171 wholesale as regulatory requirements for government contractors of all sizes?

NIST Response:
No. The federal regulation governing controlled unclassified information (CUI) is found at 32 CFR Part 2002 and promulgated by the National Archives and Records Administration in its role as CUI Executive Agent pursuant to Executive Order 13556, "Controlled Unclassified Information." The National Institute of Standards and Technology's (NIST) Special Publication 800-171 is intended to help nonfederal entities, including contractors, to comply with the security requirements using the systems and practices they already have in place, rather than trying to use government-specific approaches. It will also provide a standardized and uniform set of requirements for all CUI security needs, tailored to nonfederal systems, allowing nonfederal organizations to comply with statutory and regulatory requirements, and to consistently implement safeguards for the protection of CUI.

QUESTION 2:

Given that agencies are now using 800-171 as a requirement, will NIST update these standards to provide flexibility for small businesses?

NIST Response:
NIST updates its publications over time to ensure that the content remains current and relevant for the communities that it serves. NIST will update and maintain SP 800-171 to ensure it is clear and flexible in its use and implementation for all sized businesses, including small businesses.

QUESTION 3:

Is NIST working on any guidance or tools to make cybersecurity requirements for government contractors easier to understand and implement?

NIST Response:
NIST has provided several tools, guidance, references, and data sets to help government contractors secure their information and information systems. Examples of these include documents, such as the 800 series guidance, testing tools, commercially available validated encryption, and open source data sets to identify software assets and vulnerabilities. The NIST Small Business Corner website aggregates small business-focused resources from a variety of federal and private resources on one site: https://www.nist.gov/itl/smallbusinesscyber.

QUESTION 4:

Have you sought input on 800-171 requirements – and any changes to them – from small businesses?

NIST Response:
NIST has publicly sought input in several iterations during the creation of the draft and development of 800-171. These public calls for comments solicit feedback from government, cybersecurity professionals, industry and all businesses, including small businesses. All comments received by NIST during this open call for inputs are reviewed, adjudicated and changes are then made from draft versions to the final version.

QUESTION 5:

If so, what type of outreach have you done?

NIST Response:
NIST has a long-standing and on-going effort supporting small business cybersecurity. This is accomplished by providing guidance through publications, meetings, and events. NIST has worked with interagency partners, including the Small Business Administration, the Federal Trade Commission, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, and Federal Bureau of Investigation's InfraGard program to host cybersecurity workshops, training webinars, and has provided online resources for small businesses. NIST has

posted the documents in multiple drafts on its website. NIST has been actively asking for comments and feedback on the iterative versions of the document as it was developed and completed in its current final version. NIST held multiple webinars discussing the document, its intents and purposes, and conducted question and answer sessions during the webinars. NIST held open workshop events, meeting with industry and with government agencies to discuss the drafts as they were developed and received feedback from all stakeholders. NIST also sought and received feedback from businesses of all sizes across the country on any challenges in using 800-171 that NIST could address.

QUESTION 6:

Have you considered scaling these requirements based on the type of business, type of contract work, and type of information processed?

NIST Response:
Yes, in future versions NIST intends to scale the recommendations based on the type of information shared by the government. Planned future versions of the document will be structured to assist businesses in understanding that this scaling is to allow for different implementations and the ability to scope and tailor the use of the recommendations.

QUESTION 7:

Many small businesses are unaware of the impending threats they face from cyber attacks. Others are aware, but confused by the abundance of varying government resources available to them. Small businesses will currently find information that is presented as authoritative, current, and designed specifically for them on the websites for the SBA, FTC, FCC, NIST, DHS, and others.

How can agencies work together to ensure that small businesses are getting up-to-date and accurate cybersecurity information?

NIST Response:
Small businesses and other organizations need cybersecurity guidance, solutions, and other resources that are practical, actionable, and enable them to cost-effectively address and manage their cybersecurity risks in the context of their missions and business objectives.

Congress has given NIST responsibility through the NIST Small Business Cybersecurity Act to disseminate consistent, clear, concise, and actionable resources to small businesses. All resources are free and draw from information produced by federal agencies, including NIST and several contributors, as well as non-profit organizations and for-profit companies. The NIST Small Business Corner website aggregates small business-focused resources from a variety of federal and private resources on one site: https://www.nist.gov/itl/smallbusinesscyber.

Federal agencies continue to work together to maintain awareness of and mutually reinforce their small business cybersecurity activities. The National Cyber Security Alliance (NCSA) hosts monthly calls with federal departments and agencies including NIST, Small Business Administration, Federal Trade Commission, Department of Defense, Federal Bureau of Investigation, Department of Homeland Security, and others to exchange information about their

current and planned small business cybersecurity activities. This forum has fostered cooperation and collaboration among the participating department and agencies, allowing them to bring their subject matter expertise to activities and efforts to reach the small business community.

QUESTION 8:

Should all of these sources point back to one authoritative resource?

NIST Response:
Many federal agencies, including sector-specific agencies, engage with small businesses within their sectors of interest to provide cybersecurity resources that are aligned to and customized for use in the context of the sector's unique missions and business objectives. It is most appropriate and efficient for the departments and agencies that have the subject matter expertise in an area to develop and curate those resources.

Congress has given NIST responsibility, through the NIST Small Business Cybersecurity Act, to disseminate consistent, clear, concise, and actionable resources to small businesses. All resources are made available for free and draw from information produced by federal agencies, including NIST, as well non-profit organizations and for-profit companies. The NIST Small Business Corner website aggregates small business-focused resources from a variety of federal and private resources on one site: https://www.nist.gov/itl/smallbusinesscyber.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) leads the federal government's efforts to safeguard and secure federal civilian and private sector networks from cyber risks. CISA, works with NIST, to engage America's small businesses. CISA makes available to small businesses cybersecurity threat information, guidance on best practices, and a full range of technical assistance. These resources can be found online at: https://www.us-cert.gov/.

QUESTION 9:

Is NIST working to develop usable resources for small businesses?

NIST Response:
Yes. Congress has given NIST responsibility, through the NIST Small Business Cybersecurity Act, to disseminate consistent, clear, concise, and actionable resources to small businesses. In addition to disseminating relevant resources from federal agencies and other contributors, NIST continues to develop practical resources for small businesses by leveraging the NIST Cybersecurity Framework and other foundational standards, guidelines, and practices.

QUESTION 10:

NIST put out a request for information regarding its new "Privacy Framework," for which the comment period just ended in January. I have heard from small businesses that previous NIST guides for small businesses are overly complex and do not provide concrete, actionable steps.

How much input did you receive from small businesses for this voluntary tool that helps identify, assess, and manage privacy risks?

NIST Response:
To date, NIST has received input from small- and medium- sized businesses through a variety of formats. NIST received 81 responses to the Request for Information (RFI) it released in November 2018, on how to develop the Privacy Framework. Approximately 30 percent of the responses were from small and medium-sized businesses. Other responses to the RFI addressed the concerns of small- and medium-sized businesses and the need for the Privacy Framework to be flexible and scalable to accommodate organizations with different levels of resources and different types of privacy risks. NIST also received responses from a number of the organizations that represent small- and medium-sized businesses, including the U.S. Chamber of Commerce, NTCA: The Rural Broadband Association, Independent Community Bankers of America, and ACT | The App Association. Small- and medium-sized businesses, and the organizations that represent them, have also engaged in an initial workshop NIST held in October 2018, as well as two public webinars held in November 2018, and March 2019. As NIST continues the process of developing the Privacy Framework, NIST will continue to engage with organizations of all sizes to contribute input, including through additional public workshops, a draft framework public comment process, and sector-specific conferences and meetings.

QUESTION 11:

How do you foresee this framework helping small businesses?

NIST Response:
NIST has proposed that the Privacy Framework cover key privacy practices for managing privacy risk through an outcomes-based approach while referencing standards and guidance that can help organizations achieve these outcomes. This approach can help small businesses understand what practices comprise a robust privacy program while allowing them to determine the most appropriate means for implementing these practices. NIST anticipates that the Privacy Framework can provide small businesses with a general foundation for developing a privacy program, but additional supporting guidance may be needed to address specific concerns of small- and medium-sized businesses. NIST has had success with this approach in developing the Cybersecurity Framework, where NIST and other organizations have developed various additional resources to assist organizations of different sizes and in different sectors.

QUESTION 12:

As you craft the final framework, will you make sure that it can adjust to businesses of all sizes?

NIST Response:
NIST is developing the Privacy Framework as a living document and a tool that will be usable by organizations of all sizes, just as the successful Cybersecurity Framework has been. NIST has proposed that the Privacy Framework take a risk-based approach to allow it to be flexible

and scalable for a variety of organizations. Using a risk-based approach, rather than a rules-based approach, will allow organizations of all sizes and sectors to consider the types of privacy risks that they need to manage and adjust their resources accordingly.

QUESTION 13:

How can you revise your existing small business cybersecurity guide so that it is more user-friendly?

NIST Response:
NIST continuously seeks feedback from the community on the quality and utility of the cybersecurity and privacy resources the agency produces. NIST engages and works with small businesses and other organizations to better understand their cybersecurity needs in order to produce standards, guidelines, and other resources that are more useful to and digestible by the community. In addition to producing documentary resources, NIST is increasingly using other publication formats and distribution mechanisms such as online resources, use cases, example implementations, and video clips, to more widely share these resources and increase their utility.

QUESTION 14:

In recent years, foreign, state-backed firms have successfully breached U.S.-based security systems, obtained confidential information, and interfered with democratic systems. Since the majority of American businesses are categorized as small, this means that small business IT systems are a large part of American infrastructure that needs to be protected against cyber criminals.

What is the federal government doing to make small businesses aware of the threat of cyber-crime and to prepare them against cyber-attacks?

NIST Response:
Many federal agencies, including those with law enforcement, homeland security, and regulatory responsibilities, help to raise small business awareness of, and prepare them to guard against, cybersecurity threats. NIST's role is to raise awareness of standards and practices that can help small businesses to better identify and manage cybersecurity risks in the context of their missions and business objectives. Congress has given NIST responsibility, through the NIST Small Business Cybersecurity Act, to disseminate consistent, clear, concise, and actionable resources to small businesses. The NIST Small Business Corner website aggregates small business-focused resources from a variety of federal and private resources on one site: https://www.nist.gov/itl/smallbusinesscyber.

QUESTION 15:

How can Congress better assist you in these efforts?

NIST Response:

NIST greatly appreciates the strong support from Congress for NIST's cybersecurity efforts. NIST works with numerous House and Senate committees, including the Senate Committee on Small Business and Entrepreneurship, to educate Members and staff on the ongoing Cybersecurity programs at NIST. NIST welcomes the opportunity to continue its close working relationship with the Members and staff of the Committee as the Committee continues its efforts to address cybersecurity challenges faced by small businesses.

QUESTION 16:

There is now ample evidence that Chinese companies have used their technical products to spy on, and interfere with, American activities. Last February, FBI Director Christopher Wray testified to the Senate Intelligence Committee, in an open hearing, that smartphones made by Chinese government-owned companies, like ZTE and Huawei, have the "capacity to maliciously modify or steal information." The 2019 National Defense Authorization Act restricted federal government use of products manufactured by Chinese-based technology firms for "substantial or critical components of any system," or as "critical technology."

What is the federal government doing to ensure that it is not using these Chinese products?

NIST Response:
In accordance with Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law No: 115-232), NIST implements that provision's prohibition on use or procurement of covered telecommunications equipment or services, including any determinations with respect to telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of the People's Republic of China.

Additionally, NIST follows Department of Commerce guidance implementing Section 514 of the Commerce, Justice, Science and Related Agencies Appropriations Act, 2019, (Public Law No: 116-6), which governs certain agencies' use of appropriated funds to acquire any high-impact or moderate-impact information system, as defined for security categorization in NIST's Federal Information Processing Standard Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," and in accordance with which criteria have been developed by NIST and the Federal Bureau of Investigation to inform agency acquisition decisions.

QUESTION 17:

Is NIST working with agencies to ensure that there are no Chinese-manufactured products?

NIST Response:
In accordance with Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law No: 115-232), NIST implements that provision's prohibition on

use or procurement of covered telecommunications equipment or services, including any determinations with respect to telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of the People's Republic of China.

Additionally, NIST follows Department of Commerce guidance implementing Section 514 of the Commerce, Justice, Science and Related Agencies Appropriations Act, 2019, (Public Law No: 116-6) which governs certain agencies' use of appropriated funds to acquire any high-impact or moderate-impact information system, as defined for security categorization in NIST's Federal Information Processing Standard Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," and in accordance with which criteria have been developed by NIST and the Federal Bureau of Investigation to inform agency acquisition decisions.

Senate Committee on Small Business and Entrepreneurship Hearing
March 13, 2019
Follow-Up Questions for the Record

Questions for Ms. Elizabeth Hyman

Questions from:

Chairman Rubio

A 2018 Verizon study found that an astonishing 58 percent of cyberattacks are made against small businesses. Hacking and the use of malware are the most frequent methods that these criminals use to attack vulnerable small businesses. The government certainly has an interest in educating small businesses on practices and methods that can help reduce these devastating attacks.

QUESTION 1:

What is the government missing in the way that it is currently trying to help stop cyber-attacks on small businesses?

All of us – government and industry alike – must play a significant role in helping small businesses improve their cybersecurity. While there is not much government can do to stop adversaries from trying to attack small businesses, there is much that can be done to help mitigate risk and prevent many attacks from being successful. There are steps small businesses can and should take on their own to help create a culture of security among their employees, customers, and industry partners. I have outlined those needs in my testimony.

The area where government can do better is to provide a more unified and timely set of information that serves to help these small businesses both protect themselves from cyber threats and counter new emerging threats. The SBA, DHS, and others are helping to lead our nation's efforts in countering these threats. A unified portal for this information and more guidance tailored for small businesses that focus on best practices, threat information, and trend analysis can help our small businesses better understand and prepare.

America's small businesses want to protect their systems, their customers, and their companies. In some cases, it can be bewildering to know where to turn for assistance and thus don't have the information available or the training to understand how to best meet these goals. Industry and government have a role to play here and we look forward to working with Congress and our federal agency partners to ensure small businesses are ready to stop and mitigate cyber-attacks. Finally, we must also ensure that the government agencies tasked with helping small businesses have the necessary funds to carry out their mission.

QUESTION 2:

What can the government do to improve its service to these vulnerable small businesses?

As I mentioned in my testimony, small businesses do not always have personnel with the skills necessary to protect themselves and others when it comes to cybersecurity. This is often a matter of not knowing what skills they should look for in employees and also not having the budget to dedicate staff to cybersecurity. Data shows that small businesses are generally less prepared to counter and respond to cyber-attacks than their larger counterparts and there is always more we can be doing to equip them with the appropriate tools.

There are several things that the government can do to help small businesses protect themselves from cyber threats:

- Small Business Development Centers (SBDCs), managed by the SBA, can help identify and address the cybersecurity challenges unique to small businesses. The SBDCs should focus on improving the three key elements of modern security: technology tools, business processes, and effective employee education including vendor neutral certifications.

- Additionally, increasing the prevalence of cybersecurity advisors (also known as CSAs), who are regionally-located DHS personnel who offer immediate and sustained cybersecurity assistance to prepare and protect organizations, including small and mid-sized businesses. To maximize their help with small businesses, CSAs should be focused on helping SMB's understand how to build security policies and establish proper enforcement.

- The federal government must also maintain its robust partnership with industry. In this role, the focus should be on improved information sharing and guidance on best practices. With consistent open lines of communication, small businesses throughout the country can remain updated on the most recent threat trends and the best tools available to combat them.

QUESTION 3:

How are you working with the government to prepare small businesses?

CompTIA works with government partners on a daily basis to help improve our nation's overall cybersecurity posture. We do this by advocating for policies that will strengthen both the government and commercial workforce to combat the threats we face and promote policies that will enable and encourage innovation and the ability for businesses of all sizes to be nimble. Our member companies are committed providers of goods and services that help the government have the best line of defense against bad actors.

In addition, several years ago CompTIA was a founding member of the Cybersecurity Credentials Collaborative (C3). The mission of the C3 is to provide awareness of and advocacy for vendor-neutral credentials in information security, privacy, and related IT disciplines. In an effort to help better align federal cybersecurity job descriptions with those in the private sector, the C3 members all mapped their certifications to the NIST Cybersecurity Workforce

Framework. This framework is used by businesses of all sizes to determine what skills they need most. By helping to break down which jobs exist and the skills that are needing, we are simplifying the process for small businesses that do not have the HR and technical skill support to recruit talent.

QUESTION 4:

How can Congress help both federal agencies and private partners in this uphill battle against bad cyber actors?

In order to help both federal agencies and private partners counter bad cyber actors, Congress should prioritize efforts to strengthen our cybersecurity workforce. Regardless of whether or not we have the best technology in the world to counter these actors, if we do not have the personnel to support it, it will be meaningless. In strengthening our workforce, Congress should emphasize training that leads to vendor neutral industry-recognized certifications, as well as apprenticeships, and modifications to our K-12 education system to better prepare the workforce of tomorrow.

In helping small businesses effectively address cybersecurity concerns, we must also be sensitive to the limited resources many small businesses have to make investments. One important opportunity, which was outlined in my testimony, would be to pass a federal data breach and notification standard that eliminates the need for small businesses to comply with a complex patchwork of data breach notification laws. Simply put, this would increase security and reduce financial burdens on our small businesses.

Senate Committee on Small Business and Entrepreneurship Hearing
March 13, 2019
Follow-Up Questions for the Record

Questions for Ms. Karen Harper

Questions from:

Chairman Rubio

You previously mentioned that Congress should establish guidelines to ensure security of online data with clear and simple steps for companies to follow. You are in the unique position of being both the head of a small business and having expertise into how advanced cyber-attacks have become.

QUESTION 1:

How can the government provide practical guidance that small businesses need?

ANSWER 1:

Many small businesses in the US do not have an appreciation for the critical data that they maintain. When we talk about cyber vulnerability in the media, for example, we tend to focus on breaches of banking data, credit data, usernames and passwords for service accounts, and the like. While these can be some of the most damaging threats to the population at large, there are many other forms of data that can be vulnerable that are maintained by businesses throughout the US, large and small alike—employee data including compensation data, background check data, customer data including personally identifiable information (PII), and the like. Education and outreach to the small business community to convey the breadth of the cyber threat is currently insufficient. The Government should fund the development of more active cyber education campaigns through federal, regional, and state resources to better inform small business decision-makers about their critical role in our defense.

But, education regarding the threat is insufficient. Currently, even with a healthy understanding of the severity of the threat, small businesses are powerless to act in defense, due to the sheer complexity of the information technology (IT) infrastructure on which they operate. Small business owners and operators must also be provided with tools and guidance to do something about the threat. Simple guidance and tools must be developed (with appropriate funding) to empower small business decision-makers to take action. Federal agencies, including the SBA, must be tasked with the development and delivery of these tools through easily accessible channels to small business. Finally, the tools must be *specific* to various types of small business and cyber vulnerability profiles. General guidelines only serve to confuse. Only specific guidance, including recommended technology solutions, are actionable.

QUESTION 2:

What is the best way to tailor cyber resources to help the broadest variety of small businesses?

Businesses that contract with the government, like Charles River Analytics, have to comply with certain NIST standards. As the government seeks to bolster its cybersecurity, it requires increasingly high standards of its contractors, including small businesses.

ANSWER 2:

All small businesses, whether US Government contractors or not, carry a cyber vulnerability. The specific and actionable guidance requested in ANSWER 1 above is the first step. Small business decision-makers must be able to "see themselves" in the guidance provided. So, targeting the delivery of compliance recipes to which a small business owner can map their operation, coupled with clear technology recommendations of compliant solutions for their "class" of business, seems an appropriate step in the right direction.

QUESTION 3:

How can this Committee help organize all of the requirements that small business contractors are expected to comply with?

In your testimony, you mentioned that NIST compliance cannot currently be achieved at a minimal cost to small businesses – both in terms of man hours and in cost for IT infrastructure.

ANSWER 3:

Small business Government contractors require clear guidance on two fronts: (1) what is and is not controlled unclassified information (CUI)?; and (2) what do I need to do to be compliant?

The Committee could engage with Federal agencies to encourage/mandate clarification of the CUI question. Enforce agencies to correctly identify CUI, and appropriately mark that CUI to help us better understand our responsibility for data protection. Then, provide much clearer guidance (recipes) for NIST compliance.

QUESTION 4:

Until the private market creates NIST-compliant products, are there ways that the government can help small businesses comply with these requirements?

ANSWER 4:

This seems a matter of "carrots and sticks."

For the small business (at least the DoD contractor base), the NIST-800-171 is a "stick". We must comply to continue to do business with the DoD, even though the path to compliance

remains unclear for most of us. Are there incentives ("carrots") that could be introduced to motivate as well – tax incentives for cyber defense investments, for example?

For the commercial IT vendors, the Government, as a significant customer for most of these vendors, might provide a "stick" by setting a deadline for all US Government acquisition of IT infrastructure to be natively compliant with NIST 800-171. A "carrot" might be the federal funding of a consortium of IT vendors to provide helpful guidance to the small business community—something akin to a federally funded NIST variant of the HITRUST Alliance (https://hitrustalliance.net/about-us/), which provides guidance, tools, and frameworks supporting HIPAA-compliant medical data protection.

Statement of Dr. Richard Amos, President, COLSA Corporation, Huntsville, AL

Submitted to the United States Senate Committee on Small Business and Entrepreneurship on Tuesday March 26, 2019, Room 428A, Russell Senate Office Building

Hearing Entitled "Cyber Crime: An Existential Threat to Small Business"

Chairman Rubio, Ranking Member Cardin and members of the Committee,

COLSA Corporation would like to thank the Committee for their continuing support of small businesses and for their focus on the critical issue of Cybersecurity and its impact on small businesses. We appreciate the opportunity to comment on the record on this important issue.

COLSA Corporation has a 38 year history as a small business supporting primarily the Department of Defense and the National Aeronautics and Space Administration. COLSA is a long term provider of Cybersecurity services to these organizations, and currently has over 500 employees providing a variety of Cybersecurity services to the Unites States Government. As such, COLSA is in a good position to offer a perspective on this critical issue for the Committee's consideration.

The Committee's recent hearing, "Cyber Crime: An Existential Threat to Small Business," addressed a critical issue and provided an excellent forum for a discussion of Government's role in helping Small businesses improve their Cybersecurity posture. Small businesses are providing critical support to all parts of Government, and as such, represent a key component of the Federal infrastructure. The small business component, like others supporting the interests of the United States, is increasingly under attack from a wide variety of individuals and organizations wielding increasingly sophisticated technologies.

Starting with the Computer Security Act of 1987 (Public Law 100-235) and continuing through more recent legislation such as the Cybersecurity Enhancement Act of 2014 (Public Law 113-274), the Congress has long recognized this growing threat and has undertaken significant legislative initiatives to strengthen the nation's cybersecurity posture.

More recently, Agencies of the Federal Government have begun to provide a wide array of resources to help combat this threat. At the same time, the Cyber protection requirements for doing business with and for the Federal Government have, appropriately, substantially increased.

One example particularly relevant to the small business community is the good work done by the National Institute of Standards and Technology (NIST) in the Cyber protection arena. NIST makes a wide variety of resources available to the Federal contracting community. Resources such as the Federal Computer Security Managers Forum and the components of the NIST Cybersecurity Framework are just two examples of the exceptional resources available to

both large and small businesses to assist in increasing the Cybersecurity posture of their organizations. Additionally, NIST produces excellent industry standards, such as the Risk Management Framework and the information security guidance in NIST Special Publication 800-171 "Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations."

The Defense Federal Acquisition Regulation (DFAR) process has codified implementation of the NIST 800-171 requirements, and compliance with these guidelines is now a requirement for Department of Defense contractors of all sizes. This is a good first step, however, it should be noted that compliance with the guidelines is costly to implement. For small businesses, this implementation can be particularly daunting.

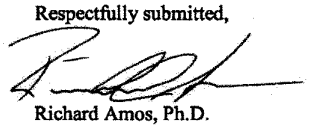
Our company is a larger small business, and we have a well-educated staff of Cybersecurity professionals. Even with those advantages, implementing all of the 800-171 requirements took time and required a large capital investment. Most small businesses do not have these advantages, and to those companies, these guidelines can represent a seemingly insurmountable barrier.

To support the continued growth of small businesses and simultaneously help enhance the Cybersecurity posture of these important components of the Federal system, the Congress should explore the development of specific managed service capabilities to help small businesses implement new Cybersecurity guidelines in a cost effective manner. For example, a cooperative of sorts could be developed and operated in a manner that allows smaller businesses to procure secure information services at a cost point which helps facilitate their entry into the Federal services market.

As technologies and threats continue to evolve, these Cybersecurity best practices and guidelines will continue to evolve and will likely be even more costly to implement. Small businesses will no doubt continue to struggle to stay abreast of this fast evolving field, and they will no doubt continue to struggle to balance the costs of improving their security posture with the other elements of building and operating a small business. Continued support from the Congress and applicable Federal organizations is essential to their continued success.

Thank you for the opportunity to submit a written statement on behalf of COLSA in support of the Government's initiatives to help small businesses improve their Cyber posture. Please do not hesitate to contact me if I can provide any additional information that could be helpful to the Committee.

Respectfully submitted,



Richard Amos, Ph.D.
President, COLSA Corporation

○