CYBER READINESS
INSTITUTE

“Strengthening the Cybersecurity Posture of America’s Small Business Community”

Testimony of
Kiersten E. Todt
Managing Director, The Cyber Readiness Institute

United States House of Representatives
Committee on Small Business

July 20, 2021

Chairwoman Velázquez, Ranking Member Luetkemeyer, Vice Chair Mfume, and Vice Ranking Member Williams, thank you for the opportunity to testify before you. I currently serve as Managing Director of the Cyber Readiness Institute, a non-profit effort that convenes senior executives of global companies to share resources and best practices that inform the development of free cybersecurity tools for small and medium-sized businesses (SMBs).

The assaults on our nation's digital infrastructure, particularly over the last twelve months, through the compromise of small and medium-sized businesses (SMBs), underscore the urgent need to close a critical gap in our nation's cyber defenses.

When we think about cybersecurity, we tend to think at a macro level – about state actors, and state secrets; about hacks of millions of online identities; about direct threats to critical infrastructure. And when we think about remedies, we tend to focus on digital giants and on national or multinational policymaking. Those policy solutions are necessary and appropriate, but they are not sufficient. The threats we face – as a nation, and as individual consumers and citizens – are not restricted to the macro level. As the saying goes, a chain is only as strong as its weakest link. Today, that chain is our economy's supply chain, and our small and medium-sized businesses (SMBs) are a weak link.

SMBs, which are constrained by limited resources and unable to invest proportionately in cybersecurity, expand our risk exposure, significantly. Eighty percent of America's businesses have fewer than 10 employees, and 95% have fewer than 100. SMBs are the backbone of our economy, but they are inherently fragile. During the pandemic, according to the SBA Administrator, a small business was closing every hour. These small enterprises lack the resilience to withstand a barrage of cyber attacks. Small businesses don't have the safety nets that large businesses do – and an attack of any size can challenge the viability of SMBs.

At the end of 2020 and earlier this year, we experienced the impact of the SolarWinds and Microsoft Exchange attacks. Earlier this year, we have also witnessed the impact of supply chain disruption demonstrated through attacks against Colonial Pipeline and JBS. More recently, we have been forced to understand that, in addition to physical supply chains, all businesses – including SMBs – must pay attention to their IT supply chain. These events have brought us to another so-called "inflection point" – "so-called" because we use this term

frequently when it comes to cybersecurity, yet we continue to fail to do what is necessary to improve America's cyber defenses. These events and attacks are symptoms of the challenges we face. Policies are not enough. Nor can we simply shrink tools and techniques employed by major corporations into compact versions for SMBs. Many SMBs are doing what the experts tell them to do – updating and patching software, changing passwords, removing malicious code—but neither they nor we can be lulled into believing that they are doing enough.

SMBs need access to cybersecurity resources and support from the federal government and need prescriptive and easy-to-adopt programs and approaches that strengthen their everyday operations. Because a small business may not have a department or even a single employee solely focused on cybersecurity, approaches grounded in creating cultural change through human behavior and education are critical to helping SMBs become more resilient. Human behavior can be a force multiplier for cybersecurity in SMBs (and larger companies, as well). SMBs must be educated on the threats and the fundamental actions they must take to be resilient.

There are multiple threats to SMBs, but ransomware, phishing, and credential-stealing (password theft) are among the most serious. These threats are only expected to grow as industries continue to take more operations online because of the changing nature of work, post-pandemic. This rapid change has led to gaps in cyber resiliency, as firms, especially those with fewer resources, struggle to keep up. These increasing vulnerabilities are being readily and frequently exploited by malicious actors.

The consequences of a cybersecurity compromise are not only relevant for the company in question but expose other businesses in their supply chain, as well. Given that over two-thirds of large businesses outsource a portion of their functions and allow third-party access to their data, insufficient cyber protection among SMBs can be consequential for larger firms, too – as we saw with SolarWinds and Kaseya. A 2020 report compiled by Accenture found that up to 40% of cyber breaches are indirect, meaning they target weak links in supply chains or business ecosystems.

Our nation's cybersecurity challenges are diverse. One foundational way we can improve our defenses is by supporting and investing in the cyber readiness of small and medium-sized businesses. America's hundreds of thousands of SMBs, mobilized, educated, and supported to

be our resilient frontline of cyber defense can become a great strength for our country. The critical investment in building that strong defense will pay major dividends.

The federal government can play a critical role. Earlier this year, the Cyber Readiness Institute released a white paper, “The Urgent Need to Strengthen the Cyber Readiness of Small and Medium-Sized Businesses: A Proposal for the Biden Administration,” outlining actions to help small businesses. Here are five steps, from the white paper, that the federal government can take today that will have expedient and measurable impacts on SMB cybersecurity defenses.

#1: Roll Out a National Cyber Readiness Education Campaign. Awareness is critical. For SMBs and the entire population, we need an aggressive, accessible and easy-to-understand nationwide awareness campaign.

As a nation, we have a long history of using public awareness campaigns to save lives and change behaviors – from forest fires to seatbelt safety, to the post-9/11 “See Something, Say Something” advertisements. Now is the time for a national awareness campaign that focuses on the role of human behavior in cybersecurity and educates everyone about the actions that will make us all secure. There is public support for a government campaign: More than 60% of the U.S. and global SMBs, in a 2021 CRI survey, believe the government should create a national public awareness campaign to promote cyber readiness.

Cybersecurity is a complex area, not easily reduced to a simple message. An effective public service campaign should focus on a single, basic cybersecurity issue – such as using multi-factor authentication, which experts assert would reduce cyber attacks, significantly. Focusing on a single topic with a simple recurring message will help protect SMBs from commonly used methods favored by hackers.

#2: Create an SMB Cybersecurity Center. A national awareness campaign focused on cyber readiness will naturally direct SMBs to a list of available public and private resources. Today, those resources are scattered across several government agencies, sometimes with advice that is too technical for many business owners who do not have an internal IT staff or who outsource cybersecurity. Given the ongoing work for SMBs by the Cybersecurity and Infrastructure Security Agency (CISA), we recommend that CISA is the agency best positioned to be tasked with the curation of cybersecurity resources for SMBs. The agency commissioned to curate resources must also have as its core mission the task of simplifying concepts surrounding cybersecurity to make them understandable and accessible to business owners.

#3: Establish Cybersecurity Incentives. To spur SMB investments in cybersecurity, the federal government should provide an incentive in the form of tax credits. The Treasury Department, in collaboration with the Small Business Administration (SBA) and CISA, should establish guidelines for SMB investment in cybersecurity to qualify for tax credits. While tax credits will reduce the amount of taxable income the government collects, improved cybersecurity will reduce the economic damage done by cyber attackers and have a net positive impact on the security, strength, and resilience of the digital economy.

Working with other agencies and soliciting industry input, Treasury can establish requirements for companies to indicate that they have taken steps to become cyber ready before receiving any tax credit. These standards should require cybersecurity training and education for employees to qualify for the credit. Education should underscore the need to create a culture of cybersecurity in the workplace. Awareness of the risks that come with cyber breaches, and behaviors that mitigate these risks, should be embedded in everyone's actions, from employees to firm leadership so that employees understand their responsibilities, and actions are taken to ensure the organization is cyber ready.

#4: Set Cybersecurity Standards. We can no longer rely on market forces or voluntary actions to improve the cybersecurity of our public and private institutions. Currently, "first-to-market" trumps "secure-to-market." Market forces prioritize profit over security – and enable vulnerabilities, which our adversaries easily expose. This structure is unacceptable and must change. We must create standards that prioritize security in the market. Aligned with an effective education and awareness campaign, market standards for security will help consumers prioritize security, as well.

Establishing standards through industry and government collaboration is vital to securing supply chains. We have successfully established regulations that improve the safety of our roads, health care, and financial systems. We should establish minimum standards for cybersecurity.

There is no one-size-fits-all solution to preparing organizations to be cyber ready. The number of employees, industry, technical knowledge, and financial capabilities are just a few factors that vary by company. But industry and government can work together to establish standards, focused on a risk management approach, that take those factors into account.

#5: Launch National Cyber Squads. A government program funded through grants awarded by the National Science Foundation already exists – CyberCorps: Scholarship for Service. That program, however, is designed to recruit and train IT professionals and cybersecurity managers for positions with federal, state, and local agencies. A new Cyber Squad program would expand the pipeline of talent available to SMBs and will also facilitate engaging different disciplines and expertise in creating cultures of cyber readiness across SMBs.

Cyber Squads can address several issues that hinder SMB efforts to become cyber ready – including a talent shortage and a lack of financial resources. A Cyber Squad program modeled after the Peace Corps or a campaign similar to the Science, Technology, Engineering, and Mathematics (S.T.E.M.) education initiative will allow students to explore an interest in pursuing cybersecurity as a career path while providing a connection with their local communities.
In cooperation with community colleges and universities, student interns with expertise in various disciplines would receive additional training in the role human behavior plays in making SMBs secure – issues such as password management, updating software, and phishing awareness – that are not addressed in many cybersecurity programs. Cyber Squads would be sent into the community to help local SMBs improve their cyber readiness. Initially, the program would focus on helping underfunded minority-owned businesses.

CONCLUSION

These recommendations and actions highlight the need for urgent public/private collaboration to address the serious vulnerabilities that put our national security and economic well-being at risk.

The cyber events of the last year demonstrate how our cyber adversaries are increasingly sophisticated in identifying our vulnerabilities and weaknesses and exploiting them. We must bolster our cyber defensive capabilities while continuing to invest in our offense.

SMBs need access to cybersecurity resources that are prescriptive and accessible. Resources, tools, and techniques for SMBs require a different approach from what larger enterprises need. The goal is the same, to create a healthy, protected company, but the path to get there is different. We cannot simply shrink the tools and techniques employed by major corporations into smaller versions for SMBs. We must be proactive in supporting SMBs to become a strength in our ecosystem, not a weakness. They must become more resilient and cyber ready to ensure our nation has a strong foundation and a culture of security.