U.S. Small Business Administration

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.