WRITTEN TESTIMONY

OF

CHRIS DERUSHA
CHIEF SECURITY OFFICER
STATE OF MICHIGAN

FOR A HEARING ON

"WHAT STATES, LOCALS, AND THE BUSINESS COMMUNITY SHOULD KNOW AND DO: A ROADMAP FOR EFFECTIVE CYBERSECURITY"

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Tuesday, February 11, 2020
Washington, D.C.

Thank you to Chairman Johnson and Senator Peters for inviting me to speak today on the subject of cybersecurity among states, localities, territories, and tribal governments. As the Chief Security Officer for the State of Michigan, this is a fantastic opportunity for me to highlight the steps we are taking to better secure our state and discuss some of the challenges we face.

It is no surprise to the members of this committee that the threat environment we face is daunting. Attacks on government organizations at all levels continue to increase and demonstrate the ever-expanding capacity of our adversaries. State of Michigan firewalls repel over 90 million potentially malicious probes and actions every day, and we are not unique. To defend our networks and the data entrusted to us by our residents, state and local cybersecurity leaders are taking proactive steps to improve protections. States are often hailed as the "laboratories of democracy." In the face of determined and well-resourced opponents, states are proving all across the country that we are test beds for cybersecurity innovation as well.

Cybersecurity in the State of Michigan

In the State of Michigan, the state government's information technology (IT) and cybersecurity are centralized under the Department of Technology, Management, and Budget (DTMB). Centralization enables the state to enforce common security policies, standards, and controls across state agencies and leverage economies of scale when procuring new technology. Benefits include a robust risk assessment and security accreditation process for all new systems and applications, the ability to apply governance and enforce security policies, standardized cyber awareness training and phishing exercises, and a common operating picture of threats facing the entire state government enterprise. In Michigan, several organizations have cybersecurity-related responsibilities, but all have different missions:

- Michigan Cyber Security (MCS): Information security for the State of Michigan is managed by MCS within DTMB. The Michigan Security Operations Center hosts advanced security capabilities such as threat hunting, incident response, digital forensics, and vulnerability management.
- Michigan Cyber Command Center (MC3): The Michigan State Police's MC3 coordinates cybersecurity-related activities as they relate to emergencies and computer-based crimes. Whereas MCS is focused on the state government's information assets, MC3's purview extends to all of Michigan.
- National Guard: Michigan is fortunate to have both Air and Army National Guard Units with cybersecurity capabilities. The State of Michigan is working closely with our colleagues in the Guard to formalize how we can operate together in times of emergency, and next month will mark the first National Guard assessment of one of a state agency's cybersecurity capabilities.
- Michigan Cyber Civilian Corps (MiC3): Designed to leverage Michigan's cybersecurity talent, the MiC3 program allows qualified cyber professionals from across all industries to volunteer their services to respond to cybersecurity events on behalf of the state.

In 2015, the state developed the Michigan Cyber Disruption Response Plan (CDRP) to delineate roles and responsibilities between MCS, MC3, and the National Guard, who all work closely together to prevent and respond to cyber events. The CDRP clearly sets forth chains of command, delineation of responsibilities, and processes for escalation, decreasing the chaos that often accompanies major security incidents. However, as I recently told a group of local officials, the value of a response plan can be significantly reduced if it is not tested. It is for this reason that the State of Michigan conducted a functional exercise this past November that simulated major compromises at two large state agencies and involved numerous senior decision makers. Armed with the results of the exercise, we are currently

updating our processes to ensure we are using best practices that reflect the realities of both our adversaries and our defenses.

Federal Assistance to the State

While the close working relationship between DTMB, Michigan State Police, and the National Guard is essential to defending the state's public and private networks, another key relationship is the one we share with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). As a former DHS cybersecurity official, I understand the tremendous resources DHS can bring to bear as well as its eagerness to do so. Michigan is fortunate to have a CISA cybersecurity liaison who helps us coordinate with our national-level partners, saving us from navigating the Federal bureaucracy on our own. By having a direct line to DHS, we are able to incorporate a Federal perspective into our decisions and better understand the resources available to us. Providing such resources to every state, as described in **S. 3207, the *Cybersecurity State Coordinator Act***, would be a major asset to state and national cybersecurity efforts by ensuring greater continuity between the efforts of states and the Federal Government. It would also provide a stronger state voice within CISA, helping them to better tailor their assistance to states and localities.

Similarly, **S. 1846, the *State and Local Government Cybersecurity Act*** would help states like Michigan access resources, tools, and expertise developed by our Federal partners and national cybersecurity experts. This includes making available to state and local governments the experts at DHS's National Cybersecurity and Communications Integration Center for training and consulting. It would also afford these organizations with greater access to security tools, policies, and procedures to help drive vital improvements.

I want to sincerely thank the Chairman, Ranking Member, and numerous members of this Committee for their bipartisan leadership on this legislation and support all efforts to see both bills be enacted into law.

Beyond the State: Securing the Digital Ecosystem

The Federal Government and most state governments operate largely decentralized models in which every department and agency must provide for itself. Under this system, some agencies build mature cybersecurity operations while others have little to no ability to defend themselves. Agencies also end up competing against each other for scarce cybersecurity professionals. The interconnected nature of the digital age means securing a system or network can no longer be achieved by simply protecting oneself. Governments at the Federal, state, and local levels interact with each other digitally every day, and improving the security of any of these levels of government require enhanced security capabilities for the others.

However, as difficult as the current environment is for states, it is even more perilous for counties and localities. As much as state IT and cybersecurity programs face shortages of human and financial resources, these are even more scarce for smaller units of government. For instance, of Michigan's 83 counties, which are home to approximately 10 million people, only three have uniquely designated Chief Information Security Officers with dedicated time and authority to address cybersecurity for their organizations. Even their websites face legitimacy challenges as few use the .gov domain, opting instead for the easier to obtain .com. .net, or .org domains. To give a sense of scale, Michigan has over 2,000 local government-affiliated entities: counties, cities, villages, townships, K-12 and higher education institutions, transit and utility authorities. In fact, there are only approximately 8.5 percent of all eligible

local governments across the country on the .gov domain, according the General Services Administration (GSA).

Understanding these challenges, I am pleased to see steps are being taken at both the state and Federal levels to help these county and local governments. S. 2749, the DOTGOV Act seeks to ease the process for these governments to obtain .gov domain names, providing the sites themselves with greater security and offering greater assurances to residents that they are, in fact, looking at a government website. The bill also charges DHS with providing information to make the transition to the .gov domain easier and provides the Director of CISA with greater authority to waive associate fees if he or she deems it necessary. Passage of S. 2749 would certainly go a long way in providing greater security assurance for local and county government websites.

The State of Michigan has also been proactive in developing new ways to provide support to county and local government systems and networks. One of these efforts was dubbed the "CISO-as-a-Service" initiative, which leveraged a centralized pool of cybersecurity experts to advise a pilot group of counties and cities on their security posture. While the results were positive for 13 communities, the model proved to be unscalable when targeting the 2,000+ local entities across the state. However, leaning on the experience gained from the pilot, we created the Cyber Partners Program. This program pulls together the IT and cybersecurity leadership of county and local governments across the state and provides a forum for combatting current challenges and disseminating best practices and information. Cyber Partners is currently piloting a new initiative that would utilize a framework of priority security controls that county and local government could use to better understand the state of their security protections, develop prioritized plans to improve their posture, and potentially, seek additional consultative assistance. While securing county and local IT is an important end unto itself, our efforts in this area have also been essential as the State of Michigan, and the country at large, prepare for the upcoming 2020 elections.

In addition to helping counties and localities improve their defensive postures, Michigan has also taken steps to help them respond to incidents when they occur. As previously noted, the MiC3 is an organization of qualified cybersecurity professionals who have volunteered their skills should an incident occur at critical infrastructure, county or local government organizations. Currently approximately 100 members strong, the group has helped numerous organizations respond to significant compromises of their systems, including ransomware attacks, and helped them reestablish operations. With members from across the state, MiC3 significantly expands Michigan's ability to secure its information landscape.

While the security of government entities, be they state, local, or otherwise, is important, our digital ecosystem is ultimately made up of individuals. Every year, the theft of personal information from Americans, including Michiganders, costs our economy billions of dollars. To combat this dangerous trend, the State of Michigan is exploring options to provide greater protections for our residents. This could include a free mobile app that would help residents secure their mobile devices from cyber criminals, reducing the potential of fraud. The app is designed not only for security, but for privacy, collecting no identifying information and even receiving the approval of the ACLU. By helping our residents become more secure, we help all levels of government become more secure as well.

Our country's state and local governments are on the frontlines of today's digital conflict, attacked daily by highly resourced advanced persistent threats, and there remains a great deal of work in order to secure the networks we rely on to provide essential services to the public. The State of Michigan greatly

appreciates the attention paid to this issue by the members of this committee and we look forward to continuing to work with you all to secure our critical infrastructure and protect our residents.