Remarks of Laura Clark to the Subcommittee on Intelligence and Counterterrorism
U.S. House Committee on Homeland Security
Michigan's Digital Ecosystem
June 28, 2022

Thank you, Congresswoman Slotkin, for inviting me to speak today on the subject of cybersecurity. As the Chief Information Officer and Chief Security Officer for the State of Michigan, I appreciate the opportunity for me to discuss with the members of this Committee the steps we are taking to secure our state.

Cybersecurity in the State of Michigan
In the State of Michigan, information technology (IT) and cybersecurity are centralized under the Department of Technology, Management and Budget (DTMB). Several years ago, both cybersecurity and physical security were consolidated into one area within DTMB known as Cybersecurity and Infrastructure Protection (CIP), which serves to secure the state and ensure the safety of the executive branch. Within CIP, there are several groups that provide external outreach to keep those within Michigan safe, further strengthening the cyber environment:

- Michigan Cyber Security (MCS) manages information security for the State of Michigan. The Michigan Security Operations Center has several advanced security capabilities including threat hunting, incident response, digital forensics, and vulnerability management. The Risk, Compliance and Delivery division assumes responsibility for the process, tool, and governance of security process plans and security awareness campaigns, and developing and enforcing security policies, standards, and procedures for the enterprise to follow. Security architects establish the target security and infrastructure architecture for security platforms, implementing frameworks and solutions to keep the enterprise secure.
- Michigan Cyber Civilian Corps capitalizes on the cybersecurity talent within Michigan to allow qualified technical cybersecurity professionals and experts to volunteer to respond to cybersecurity events and incidents on behalf of the state. By participating in the MiC3, members receive training to further increase their knowledge and skills and can participate in statewide exercises, encouraging outreach between cybersecurity-minded individuals.
- Michigan Cyber Partners is a collaboration between divisions at the State of Michigan, local public entities across the state, federal agencies, and national non-profits to work to strengthen and improve cybersecurity. Michigan Cyber Partners offers members the ability to share information and threat intelligence with one another, participate in statewide exercises and formal annual training offered to local government and K-12, and offers program oversight for risk assessments and federal grant programs.
- Michigan Secure is a first-of-its-kind, free statewide mobile protection app for residents. Michigan Secure protects users from cybercriminals and potential dangers encountered in the digital mobile world. The app was designed with security and privacy at the forefront, collecting no user data or identifying information.
- Resident Tooling is an effort to elevate the existing State of Michigan cybersecurity website and provide various cybersecurity information and resources to equip residents with the knowledge they need to stay safe in the online world.

Additionally, organizations that DTMB partners with who have a critical role in maintaining a safe cyber environment across the state:

- Michigan Cyber Command Center (MC3) is housed within the Michigan State Police and coordinates cybersecurity-related activities as they pertain to emergencies and computer-based crimes, extending beyond government information to reach all of Michigan.
- National Guard has both Air and Army National Guard Units with cybersecurity capabilities, in which the State of Michigan works closely with the Guard to formalize the process of working together in the event of a cyber emergency.

To aid in the distribution of roles and responsibilities between MCS, MC3, and the National Guard, the State of Michigan has developed the Michigan Cyber Disruption Response Plan (CDRP). The CDRP details chain of command, responsibilities, and processes for escalation, serving as a plan to weaken the unknown and panic that often coincides with major incidents. To guarantee the effectiveness of the CDRP, involved agencies and partners participate in workshops to review the CDRP and relative responsibilities and engage in functional exercises that simulate various scenarios and incidents that advance in severity. In completing workshops and exercises, we can ensure that proper action and best course of action is taken in the event of a cyber incident.

The Cyber Disruption Response Team (CDRT) is currently being utilized as a result of ongoing geopolitical situations, with several meetings to share the latest information occurring throughout the week that allows for the consolidation of information sharing and the streamlining of sources while offering efficiency in the consumption of information. The frequent communications have established clear triggers for the escalation of an incident and the implementation of primary and alternative communications plans through various platforms, including Microsoft Teams and HSIN.

Federal Assistance to the State

Consistent working relationships within the State of Michigan between MCS, MC3, and the National Guard are crucial to defend the state's digital landscape, and the relationships we have with our federal partners is also highly valuable. The Department of Homeland Security's (DHS) Cyber and Infrastructure Security Agency (CISA) has brought forth several resources to assist in securing Michigan's landscape. Through our CISA cybersecurity liaison, we have a direct line of communication with DHS who offers the federal perspective to assist in the decision-making process. We also have contact with the Federal Bureau of Investigations (FBI), which shares valuable information on cybersecurity events and topics to ensure we protect the state.

Additionally, the ***Infrastructure Investment and Jobs Act (IIJA)*** will be a major asset to cybersecurity efforts across the state to further secure the digital environment. With an estimated $24 million being allotted to Michigan over the course of four years, Michigan's digital landscape has the ability to be transformed. The State of Michigan has developed a cybersecurity planning committee comprised of cybersecurity experts in various fields and locations to assist in determining how the distribution and use of the allocation of funds would best strengthen the digital ecosystem across the state while securing the state and local governments, schools, and entities. Federal partners have been directly engaged in the information sharing surrounding IIJA, participating the meetings and communications plans to provide key insight on the funding and state of cybersecurity.

Beyond the State: Securing the Digital Ecosystem

The transformation of the digital environment has resulted in federal, state, and local governments being intertwined and relying upon with information sharing to help secure the ecosystem. Levels of government interact daily to improve the digital security of various environments while encountering challenges faced by human and financial resource shortages. The diversity in resources within these levels of government needs to be considered when addressing improvements to Michigan's digital landscape. For example, Michigan has 83 counties, 276 cities, 257 villages, and 1,240 townships. The population and available resources vary between these areas, resulting in an array of differing needs, improvements, and focuses across each level.

To assist in addressing the needs of local public entities and further secure Michigan's digital ecosystem, the State of Michigan, through the Michigan Cyber Partners program, offers the ability to contract for an independent cybersecurity risk assessment. The multiple pre-qualified vendors offered by the state were selected through a competitive request for proposal process, allowing entities to work with a vendor to complete assessment, planning, and coaching services to further strengthen their digital environments.

The findings of the risk assessments will assist in establishing a baseline for Michigan's plan for IIJA cyber implementation , indicating which improvements should be made with the funding to enhance security levels. Recommendations of transitioning to .gov domains for county and local governments, implementing multi-factor authentication across entities, and offering security awareness programs are being considered to further secure the state's digital environment. These items, among other options, are associated with the funds appropriated through IIJA, offering opportunities for entities beyond what they may typically have the funds to support. This reveals the need for sustainable funding post IIJA, as recipients may select a short-term benefit rather than long-term due to lack of budgetary funds. Securing the ecosystem needs to be a continuous effort, not a short-term solution.

The State of Michigan's external outreach programs also assist in securing the ecosystem. The MiC3 and Michigan Cyber Partners programs encourage discussion among cyber professionals, government entities, and educators, equipping them with the community and information needed to further secure the digital environment. The Michigan Secure app ensures that residents are kept safe on their mobile devices, and the elevation of the external cybersecurity website provides residents with additional resources to keep them safe online. The Michigan Cyber Summit, an annual cybersecurity conference available to the public, also offers valuable information sharing through its speakers and panels, providing insight on current cybersecurity topics from various perspectives.

The digital ecosystem is dependent upon governments, entities, and citizens working together to maintain and secure a safe environment. I would like to thank the Legislature and Governor Whitmer for their bipartisan support and recognition of the importance of cybersecurity, as well as the members of our Michigan congressional delegation who continue to make cybersecurity a priority, especially those who voted for IIJA and its funding support. With new threats emerging each day, it is crucial that we strive to protect our state. The State of Michigan greatly appreciates the members of this committee highlighting the importance of the digital ecosystem, and we look forward to continuing to work with you to secure it and protect residents.