U.S. House Committee on Homeland Security

Subcommittee on Intelligence and Counterterrorism

Combatting Ransomware: From Our Small Towns in Michigan to DC

D/F/Lt. James Ellis

June 28, 2022

Thank you, Subcommittee Chairwoman Slotkin, Congresswoman Jackson Lee, and the members of this committee for gathering us here today to discuss this issue of crucial importance to the State of Michigan and the nation. My name is Detective First Lieutenant James Ellis, and I am the Commander of the Michigan Command Center within the Michigan State Police.

Michigan State Police - Cyber Section

The Michigan State Police (MSP) Cyber Section, referred to as "MSP Cyber", is within the Intelligence Operations Division of the MSP and works in conjunction with the Michigan Intelligence Operations Center. Let me establish a foundation of how the MSP fits into cybersecurity as a state police law enforcement organization, with Michigan critical infrastructure, the public, and our close partners, the Department of Technology Management and Budget (DTMB) and the Michigan National Guard.

MSP Cyber is a full-service criminal investigation section responsible for investigations spanning the entire criminal file class hierarchy. MSP Cyber members are in the field pursuing active investigations from initiation and investigation to prosecution, arrest, and court testimony. MSP Cyber supports all MSP troopers and field members along with the other 580+ law enforcement agencies in the state and others nationally requiring cyber related investigative assistance, as cybercrime has no state line boundaries. As our case load continues to increase year after year, it is becoming very difficult to name a crime that does not involve technology of some kind that may contain digital evidence supporting that crime.

Services performed by MSP Cyber include but are not limited to:

- Criminal investigations both originating and assisting in an undercover capacity – over 4000 cases per year, assisting over 340 police agencies last year in Michigan
- The forensic recovery of digital evidence used for prosecution or acquittal
- Street level and electronic surveillance
- Search warrants – over 400 hundred per year; both administrative and on-scene with physical device and digital evidence seizures
- Often receiving and seizing over 1000 devices per month for forensic examination and recovery of digital evidence
- Provide expert courtroom testimony
- Provide community outreach and presentations covering all cyber/computer related topics from prevention and awareness to incident response and cybersecurity best practices

- Provide law enforcement with cyber, computer crime, and digital evidence related education and training
- Collaborate with critical infrastructure regarding information sharing and incident response
- Conduct cyber assessments for public and private industry/businesses
- Conduct criminal investigations involving the sexual exploitation and trafficking of children including the rescuing of children from sexual predators
- Investigate hundreds of cybersecurity related network intrusions and breaches of Michigan businesses annually
- Sourcing new initiatives for the MSP and the State of Michigan related to data security, privacy, policy, and compliance
- Develop and submit legislative language and provide testimony for new and modified Michigan laws regarding cybersecurity

We work collaboratively with all other law enforcement, public/private sectors, critical infrastructure, small/medium/large businesses, local, state, and national government organizations, local community groups, and citizens.

MSP Cyber is comprised of over 100 highly trained and specialized members consisting of both uniformed detective troopers and sergeants, officers, cyber analysts, dark web analysts, digital forensic analysts, incident response teams, an FBI Cyber Task Force member, a Homeland Security Investigations (HSI) Dark Web Task Force member, Michigan Department of Corrections staff members, National Guard members, two cyber trained K9 dogs, and many other support staff.

MSP Cyber Organizational Units

MSP Cyber consists of three organizational units that work in collaboration and provide overlapping services that include the Computer Crimes Unit (CCU), the Internet Crimes Against Children (ICAC) Task Force, and the Michigan Cyber Command Center (MC3).

Computer Crimes Unit (CCU)
Created by necessity in 1999 when computer technology was being used in the commission of crimes and the Internet was thought by some to be a fad. The CCU is the premier statewide leader in responding to and investigating high technology crimes and providing digital forensic evidentiary data recovery assistance to local, county, and state law enforcement agencies. The CCU operates multiple digital forensic offices throughout Michigan for the purposes of digital forensic examination and analysis.

Internet Crimes Against Children Task Force (ICAC)
The ICAC Task Force is a collection of state, local, and federal partners concentrating on child sexually abusive material (CSAM) and child sexual exploitation and trafficking investigations. MSP Cyber has the responsibility to train local law enforcement in the proper acquisition and examination of digital forensic evidence. Currently, over 50 federal, state, and local law enforcement agencies supply dedicated officers to investigate ICAC cases, with most of them working directly out of MSP Cyber offices. MSP Cyber also receives all Michigan cyber tip investigations that are reported by the National Center for Missing and Exploited Children (NCMEC) located in Washington DC. In 2021, the MSP Cyber received 11,416 cyber tips, averaging almost 1,000 investigations per month

Michigan Cyber Command Center (MC3)
Established in 2013 by necessity to coordinate cybercrime incident response and investigate the proliferation of networked information system-based crimes affecting Michigan. The MC3 is a leading resource for cybersecurity, cybercrime awareness and prevention, and cyber related network intrusion criminal investigations for critical infrastructure; federal, state, and local government entities; other public and private sectors, and citizens of the State of Michigan.

- Primary investigations include:
  - Network intrusions and breaches; unlawful access, hacking, theft, and exfiltration of data
  - Extortion and Cyberterrorism
  - Dark Web and Cryptocurrency
- Malware identification, research, analysis, origin, indicators of compromise for awareness/prevention
- Provide cybersecurity assessments, industry best practices, and recommendations
- Information sharing; breach notifications, development, and dissemination of various intelligence products; podcasts, presentations, media events, news releases
- Partnerships and collaborations – national, state, and local; FBI, HSI, USSS, DHS, and others

<u>Michigan Cyber - State Partnerships</u>

MSP Cyber, DTMB's Michigan Cyber Security (MCS), Michigan Air and Army National Guard, and many others along the way have had a long-standing collaborative partnership of almost ten years with the purpose of ensuring the cybersecurity posture through prevention and response within the State of Michigan. Together we have been a role model for many other states and major cities across the United States, who hope to replicate what we have done as a state when it comes to securing the state through prevention and response, not only within state government, but in addition to the many relationships we have created within our public and private partnerships across Michigan.

Michigan was one of the first states to create a state level Cyber Disruption and Response Plan that contains the framework and details related to responsibilities and roles that covers how to manage a state level cyber disruption, that has been used across the nation as a template, since the original version was finalized almost a decade ago. We have partnered to develop and fuel many initiatives that include the Michigan Cyber Civilian Corps (MiC3), Michigan Secure App, Cyber Partners Group, Chief Security Officer (CSO) cabinet meetings, and many more, bringing everyone together to discuss cyber and reinforce information sharing, creating multiple plans, exercising those plans, education, awareness, prevention, compliance, knowing who to contact.

We participate together in multiple cyber exercises, workshops, symposiums, and presentations, every year and involve federal partners DHS, FBI, others within Michigan from critical infrastructure sectors including Healthcare, Finance, Energy, Water, Education, and Government to assist in ensuring the cybersecurity of our water treatment plants, energy producing facilities, financial institutions, academia information systems, election systems, and others. On almost a daily basis we are sharing cyber threat detection, prevention, awareness, and recovery information among the many partnerships that have been developed to ensure the best possible cybersecurity protections are in place.

Thank you for your time and this opportunity to share our experiences in Michigan, and I look forward to addressing any questions you may have for me.