March 23, 2022

The Honorable Martin Causer
House Majority Policy Committee
147 Main Capitol Building
Harrisburg, PA, 17120

Dear Chairman Causer and Members of the House Majority Policy Committee,

My name is Zackery Mahon, and I am the area manager for cybersecurity services at Motorola Solutions. I am truly honored to appear before the Committee and thank you all for the opportunity to testify today.

Motorola Solutions is the global public safety technology leader and builds innovative solutions for law enforcement, fire, EMS, 9-1-1, and other state and federal agencies. Our commitment to delivering the best products and services for the public sector, and focusing on cybersecurity, gives us direct insight into the cyber threats that challenge first responders worldwide.

Cyber intrusions in the public safety space have grown in frequency and complexity, impacting our first responders' day-to-day operations and the communities they serve. Nation-states, criminal groups, and standalone threat actors continue to ransom our customer's mission-critical systems and prohibit them from performing emergency services. We are aware of over 400 cybersecurity attacks to state, local, tribal, territorial governments within the last three years, and we assess that it's likely many more attacks have gone unreported.

My testimony focuses on cybersecurity threats to Public Safety Answering Points (PSAPs) and Land Mobile Radio (LMR) used by state, local, territorial, and tribal governments. I will also provide options to help secure these systems for this Committee to consider.

## CYBERSECURITY ATTACKS ON PUBLIC SAFETY INFRASTRUCTURE

First, I would like to address threats to Public Safety Answering Points (PSAPs) and the key technologies being used by dispatchers supporting public safety. PSAPs are centers that process

emergency calls and help with dispatching the emergency personnel to a location. These centers use technologies like 9-1-1 call handling solutions and Computer-Aided Dispatch to perform these tasks. This critical infrastructure enables emergency responders to be informed of and respond to significant events affecting the public and its citizens.

***9-1-1 Call Handling Attacks***

When considering threats to 9-1-1 call handling systems, one of the most significant threats to PSAPs is Telephony Denial of Service (TDoS) attacks via physical and IP-based telephony lines. This type of attack floods the PSAPs and call handlers with fake calls and disrupts their ability to address genuine emergencies from citizens within our communities.

It is relatively simple for an attacker to conduct a TDoS attack on PSAPs since it only requires an arbitrary, but often high, number of phones or access to a virtual telephony system capable of making many calls at once. In either scenario, the attacker can leverage these devices by having them dial emergency numbers all at once and overloading the call handling system used by the PSAP.

The other concerning aspect of TDOS attacks against PSAPs is that threat actors could position calls when defenders cannot proactively respond due to high call volume or low staffing. These high call volume times usually occur during Statewide protests, natural disasters, and other events. Additionally, times like off-hours and some holidays can mean fewer dispatch personnel at work. Either of these situations will worsen the disruptive effects of TDoS attacks.

***Computer-Aided Dispatch Attacks***

Another technology leveraged in PSAPs is Computer-Aided Dispatch (CAD). These systems are mainly used to direct emergency personnel from police, fire, and EMS departments to the locations of an incident. Dispatchers also use CAD systems to identify first responders' location status and share valuable information about the citizens involved in the dispatching effort. More specifically, the data that is often provided and shared with first responders is the location of the caller, any relevant health issues, and criminal history. As you can imagine, this system is invaluable to effectively respond to an event and inform first responders of risks before they perform their responsibilities.

CAD systems are valuable targets for cybersecurity threat actors due to the sensitive data the system uses and the response it helps support. Ransomware is the most common threat to CAD systems. Ransomware is a form of malware that encrypts files on a device and makes the system and the systems that rely on it unusable. Malicious actors then demand ransom in exchange for decryption. They often threaten to sell or leak the victim's data if the ransom is not paid. Like many technologies we use daily, these systems become more exposed as our physical and digital infrastructure increasingly converges.

Attacks on CAD systems are occurring due to two main reasons. The first is that threat actors successfully attack this system through jointly shared network connections maintained by police, county, municipality, and state organizations. These teams often work together to provide and share data used in the CAD system to respond to events. The shared network connections are the backbone of the CAD network, which attackers often use to find their way into these CAD environments. The second way threat actors are successfully ransoming these systems is through CAD workstations that are connected directly to the public internet, a non-standard practice that is not recommended.

***LAND MOBILE RADIO ATTACKS***

LMR allows push-to-talk two-way communication between radio transceivers. While many people think of radios as just handheld devices, they are complex machines used by police, fire, and EMS during response efforts, and require vast infrastructure to support the communications. This system supports public safety mission-critical communications and private communications for commercial industries, such as oil and gas, and allows for secure and instant communication.

The most common attacks Motorola Solutions is witnessing against LMR systems are Broadcast-Denial-of-Service (BDoS) and ransomware threats. Threat actors use BDoS attacks to broadcast messages over the radio system. This type of attack often limits the ability of the first responders to transmit or receive valuable information during an emergency response effort. We saw this type of attack occur when local governments enacted curfews, and citizen-led protests were ongoing, especially during the summer of 2020. It is highly likely that these BDoS attacks were conducted in direct response to widespread protests and were ideologically motivated.

Again, threat actors are also targeting LMR systems with ransomware attacks. Due to the LMR transition to IP-based configurations, many systems are not wholly isolated from the internet. Attackers are leveraging these unknown connections to find their way into the surrounding networks of the radio system and comprising assets that are supporting radio communications. The most common issues that allow the threat actors to compromise the systems successfully are through misconfigurations, and default passwords that allow a patient or persistent attacker access in rare instances.

## CONSIDERATIONS

With this context in mind, Motorola Solutions offers two recommendations for this Committee to consider.

***Establish a cybersecurity baseline that applies to public safety systems***

First, public safety systems like the ones mentioned above are becoming more prone to attacks because the essential cybersecurity tools and processes are not required in many buying procedures.

By standardizing and determining a baseline set of requirements for cybersecurity across these systems, the opportunity for threat actors to be successful will be limited. While the state may consider its baseline, there are many cybersecurity standards and frameworks, such as the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) Cybersecurity Frameworks that organizations can quickly adopt to understand their existing gaps and priorities to secure their systems.

***Share cybersecurity threat information across state agencies and public safety environments to limit the impact to connected systems***

Cyber threats are increasing in scope, scale, and complexity. While some agencies and organizations' defensive capabilities may be strong, there will inevitably be a time when an organization is experiencing a breach. When this occurs, sharing information with surrounding agencies and public safety organizations will be critical to limiting damage. We propose that this Committee considers centralizing and sharing threat information across the state agencies and public safety organizations to proactively defend against the existing threats and reduce the overall damage to connected systems. Our team is committed to sharing our resources to help accomplish this mission.

## CONCLUSION

Once again, thank you for the opportunity to testify. Public safety environments within state, local, tribal, and territorial governments face serious security challenges ahead of ever growing cybersecurity threats. My team at Motorola Solutions and I stand ready to support your Committee with any information, recommendations, or guidance we can provide around cybersecurity services for the state, public safety, and our communities.

Sincerely,

Zackery Mahon

**Zackery Mahon**
Area Manager
Cybersecurity Services