Persistent disruptive cyber activity impacting U.S. public safety mission-critical services

Multi-State Information Sharing & Analysis Center® (MS-ISAC®)[1] & Public Safety Threat Alliance (PSTA)[2] joint report

Disclosure Protocol: CLEAR: Disclosure is not limited
Date of Writing: June 2025

The MS-ISAC and Motorola Solutions PSTA analysts assessed data for 2024 with impacts to the U.S. public safety sector.[3] This report also includes several incident examples from 2025 to demonstrate continued trends. PSTA maintains specific data on public safety mission-critical communications technologies including dispatch, public safety radio, and 9-1-1 call handling, as well as associated IT systems. PSTA tracks tactics, techniques, and procedures, as well as attacks resulting in actions on objectives. The MS-ISAC Cyber Threat Intelligence (CTI) team collects data across Albert[4] Network Intrusion Detection System (NIDS) detections, reported incidents, Cyber Incident Response Team (CIRT) cases, and Endpoint Security Service (ESS)[5] detections across enrolled state, local, tribal, and territorial (SLTT) government organizations. For the purposes of this report, PSTA includes municipal and federal cyber incidents among public safety incidents due to the high volume of cyber threat actors (CTA) pivoting beyond the initial victim to public safety partners.

Key findings

- Public safety agencies must maintain technologies with extremely high availability requirements and protect highly sensitive data. These conditions place added pressure on defenders when responding to and recovering from cyber incidents.
- Cyber disruptions of mission-critical U.S. public safety systems continue to impact the sector due to a combination of growing CTA capabilities, awareness of these systems, and increasing interconnectivity between mission-critical and enterprise IT environments.
- Credential abuse, vulnerability exploitation, and exploitation of remote services are the most likely initial access tactics, techniques, & procedures (TTPs) to impact public safety mission-critical systems.

---

[1] https://www.cisecurity.org/ms-isac

[2] https://www.motorolasolutions.com/en_us/public-safety-threat-alliance.html

[3] For the purposes of this report, PSTA defines public safety as an entity primarily engaged in activities related to the safety and well-being of the general public, including law enforcement, fire departments, emergency medical services, and other organizations that protect and serve the public in matters of safety and security.

[4] https://www.cisecurity.org/services/albert-network-monitoring

[5] https://www.cisecurity.org/services/endpoint-security-services

Executive summary

Over the last year, opportunistic CTAs have increasingly engaged in disruptive attacks against U.S. public safety mission-critical systems, affecting emergency communications and downstream operations. In 2024, 326 cyberattacks impacted municipalities, law enforcement agencies, and other public safety organizations. While overall attacks against public safety fell 12%, PSTA observed a 60% increase in attacks against mission-critical technologies[6] such as public safety radio,[7] computer-aided dispatch (CAD),[8] and public safety answering points (PSAPs).[9]

PSTA assesses this shift is likely due to CTAs developing greater understanding of and ability to disrupt mission critical technologies. These attacks have degraded emergency communications and inhibited the efficiency of first responder operations. Improper security configurations across public safety remote access devices, logins, as well as unpatched systems have further enabled this trend. To better secure systems against persistent malicious cyber activity, defenders should maintain awareness of key CTA tradecraft and implement corresponding security measures described in this report.

[6] For the purposes of this paper, the authors refer to LMR, CAD, and PSAPs collectively as "mission-critical systems"
[7] https://www.motorolasolutions.com/en_us/solutions/what-is-lmr.html
[8] https://www.dhs.gov/publication/cad-systems
[9] https://www.911.gov/issues/ng911/

Analysis

CTAs' maturing awareness and capability to disrupt mission-critical systems place strains on public safety agencies' ability to administer essential services. In 2024, Motorola Solutions' Public Safety Threat Alliance documented 24 successful cyberattacks that rendered emergency communications systems completely unavailable, disrupting critical public safety operations. Among these, ransomware was the most common attack type, resulting in agency downtime and degraded emergency response capacity.

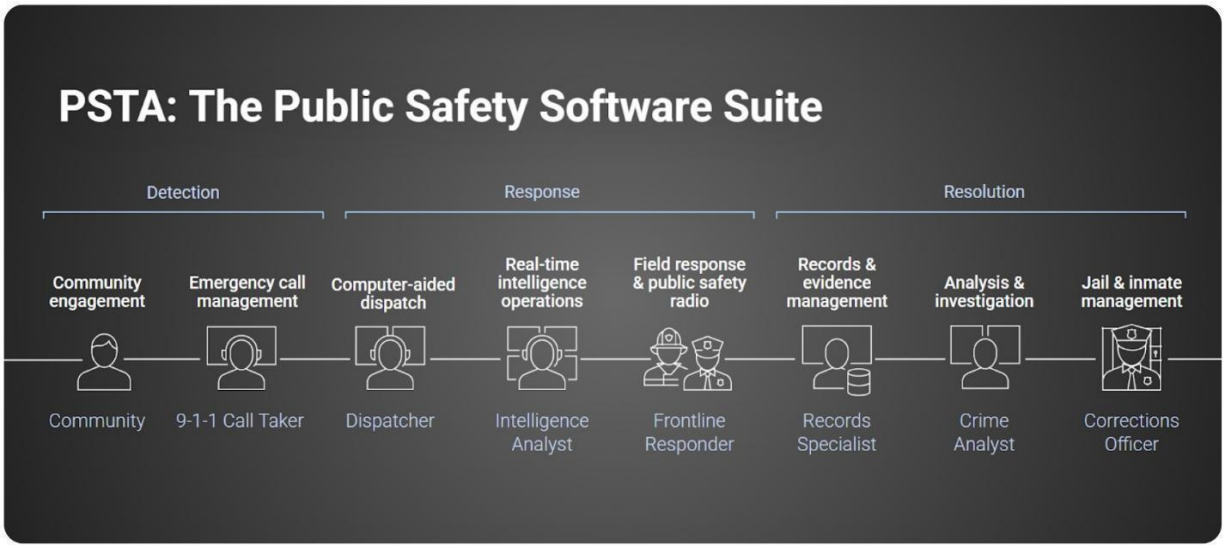


Figure 1: Depiction of how public safety radio, dispatch, and 9-1-1 exist within a broader ecosystem

Computer-aided dispatch

During this period, PSTA observed a 100% increase in CAD disruptions over the previous year. 18 cyberattacks impacted CAD systems in 2024, averaging 15 days of downtime but were limited to seven when defenders proactively disabled these systems. Several cyberattacks that shut down CAD systems also disrupted public safety radio and/or public safety answering point (PSAP) systems in 2024. Motivated CTAs demonstrated the ability to use basic tradecraft, such as credential abuse, to cross firewall boundaries from enterprise IT networks to access environments containing CAD servers and virtual machines. Additionally, in some cases CAD workstations are installed on municipal or law enforcement IT networks, increasing the likelihood of dispatch disruptions during opportunistic attacks to police and municipalities.

Public safety answering point

CTAs also disrupted PSAPs directly. In 2024, the PSTA identified five cyber incidents that impacted PSAPs. In one example, a telephony denial of service (TDoS) against a third-party service facilitating 9-1-1 call handling resulted in five hours of disruptions. The attack caused over 20 public safety

agencies to face "difficulty hearing callers and call-takers, [and] missing location information," according to local sources.

Public safety radio

Against public safety radio, PSTA observed four ransomware incidents, up from one observed attack in 2023. In a 2024 compromise of a Kansas public safety entity, CTAs conducted a brute force attack to access the victim's virtual private network (VPN) connection lacking multi-factor authentication (MFA) before deploying ransomware. This disrupted 100% of first responder communications throughout the day until the department managed to deploy a "communication on wheels" state backup system, which enabled defenders to maintain emergency response operations.

Downstream impacts

Cyber disruptions can cause impacts beyond emergency dispatch or communications. A municipality in late February 2025 declared a state of emergency following a cyberattack that inhibited their ability to share and receive mobile data inside police vehicles. Ransomware incidents often force departments to make difficult financial decisions, weighing the cost of rebuilding systems versus paying a ransom to decrypt systems. In a 2024 example, a municipality was forced to pay attackers $1.5 million out of their reserve funds to recover impacted systems after the CTAs accessed and encrypted the agency's CAD, IT, and jail systems.

A September 2024 cyberattack against a southern municipality resulted in disruptions to CAD, public safety radio, and 9-1-1 call-handling. Attackers accessed servers hosting broadband radio software as well as dispatch servers and workstations, forcing defenders to isolate and wipe the systems. 9-1-1 call recording software also went offline while dispatchers resorted to backup radios to communicate with first responders.

Cyber incidents impacting mission-critical communication technologies have also placed added strain on departments during crises such as weather events. Departments acknowledged these challenges in a recent Police1 survey,[10] which found that 85% of surveyed first responders believed disruptive events including electric grid failures, hurricanes, and wildfires threaten to overwhelm public safety departments. Three of four observed CAD disruptions impacting Florida public safety entities in 2024 occurred between August and the end of September. During this time, both Hurricane Debby and Helene struck the coast, and at least one public safety entity with a CAD disruption was in the direct path of one of the hurricanes. During CAD disruptions, departments

[10] https://www.police1.com/police-products/police-technology/publicsafetysoftware/new-2025-u-s-public-safety-trends-report-reveals-first-responders-are-embracing-ai-concerned-about-cybersecurity-and-want-to-improve-efficiency-with-modern-tech-systems

must resort to coordinating dispatch calls through pen and paper, which PSTA has observed is slower and lacks the critical context automated systems provide.

CTA tradecraft

Across all global sectors, financially motivated, opportunistic CTAs remain the biggest cyber threat, according to Google's M-Trends 2025 report.[11] In the public safety sector, CTAs take advantage of extensive remote services and improperly segmented technologies by using common attack vectors to burrow into networks and access sensitive data. PSTA observed credential abuse, vulnerability exploitation, and exploitation of remote services as the most likely initial access TTPs to impact public safety mission-critical systems.

PSTA has observed adversaries pivoting from backbone network infrastructure[12] to standalone mission critical networks. In 2024, 83% of PSTA-observed CAD attacks either began on municipal or police networks or were indirectly impacted due to attacks on those systems. For example, in July 2024, the Embargo extortion syndicate used undisclosed means to access the network of a police department before moving laterally to connected municipal and CAD networks, encrypting dispatch servers and data backups.

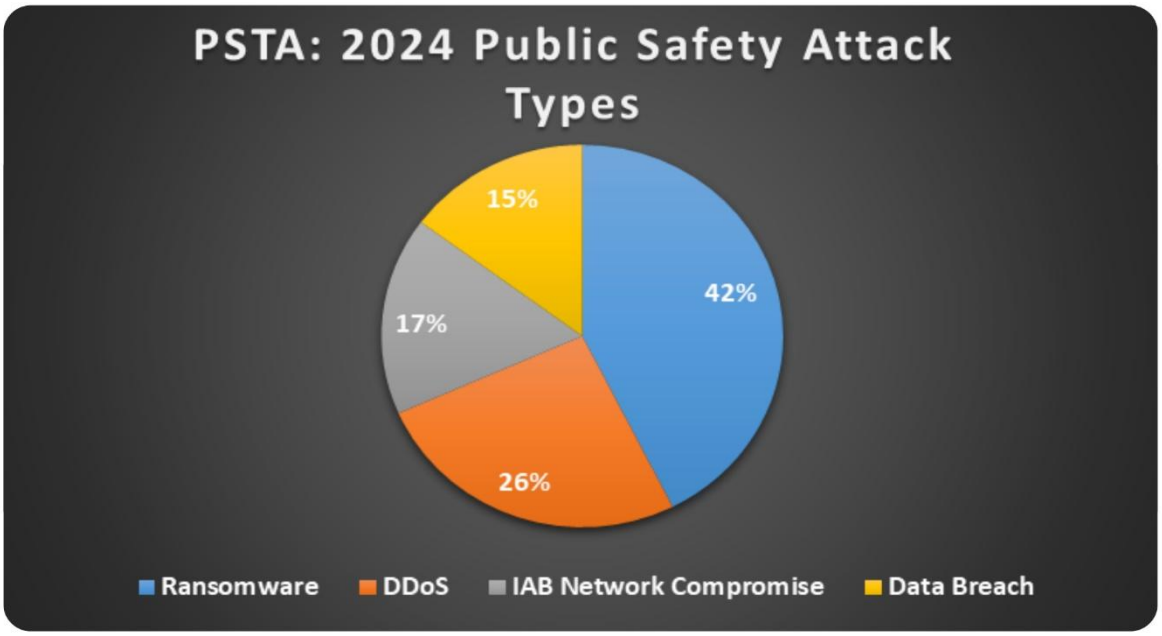


FIGURE 2: Top successful attack types impacting public safety entities in 2024

[11] https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025/

[12] A backbone network is the foundational infrastructure on which all network players deploy their services for users. For the purposes of this paper, this refers to foundational municipal infrastructure that does not directly host the mission-critical appliances.

U.S. public safety and emergency service entities were among the top five ransomware victim sectors reported to the MS-ISAC in 2024 (see Figure 3 below). Additionally, incidents against municipal and county networks often disrupt public safety and emergency services entities, so these figures likely do not reflect the total ransomware impact to the public safety sector.

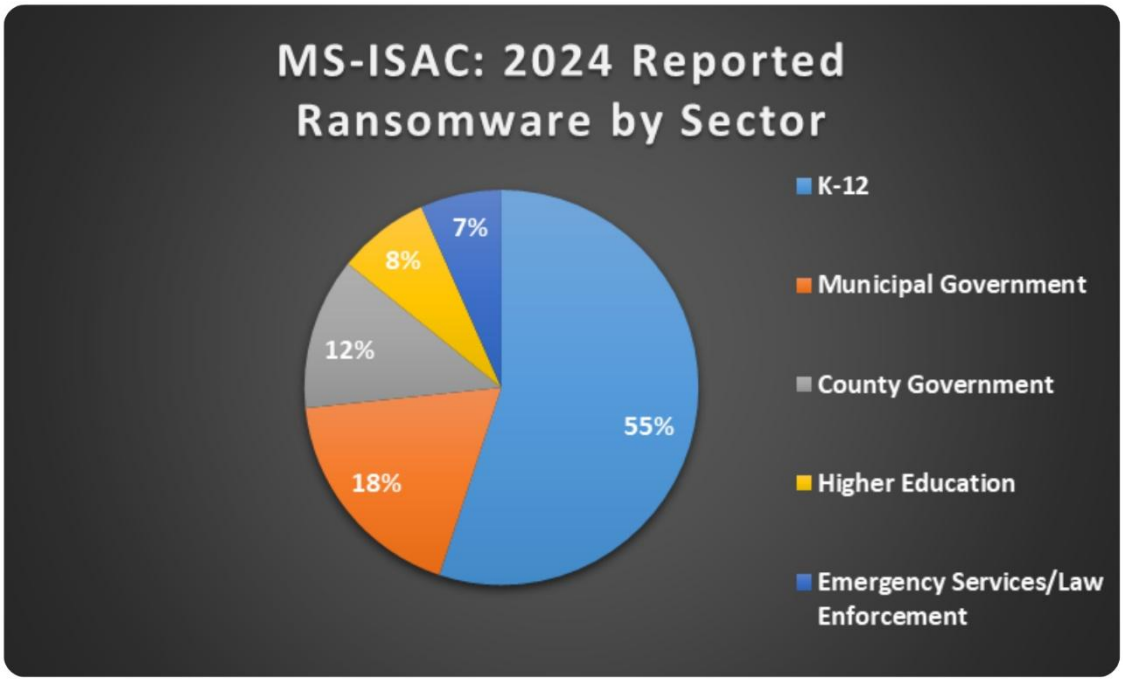


FIGURE 3: Ransomware attacks viewed across top public sector organization types

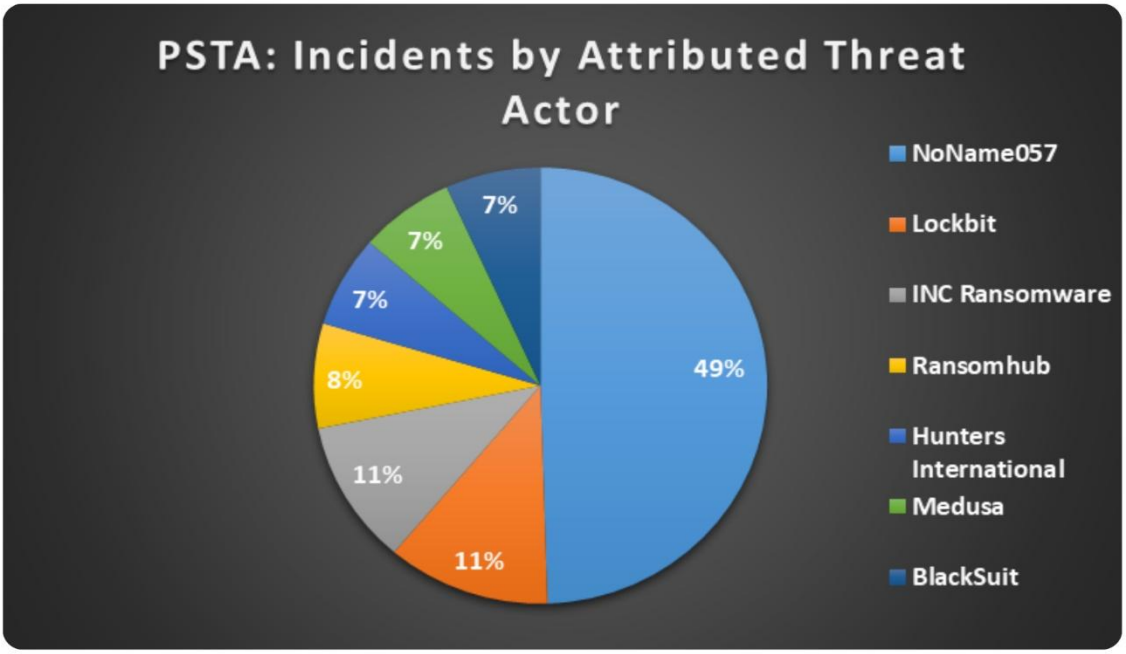


FIGURE 4: Top attributed CTAs behind confirmed public safety cyberattacks

Vulnerability exploitation

CTAs will often scan target systems for known vulnerabilities to attain initial access. In March 2024, a CTA conducted several NMAP scans using an internal IP address against a southern department's PSAP network. The IP in this case targeted port 902, which is associated with ESXi management. The IP was not associated with a defender-controlled authorized scanner, suggesting malicious activity.

PSTA also observed a CTA using a U.S. County network's internal IP to attempt to exploit 'Zerologon' (CVE-2020-1472)[13] against a connected public safety radio system. In February 2025, unknown CTAs similarly attempted to exploit CVE-2025-1094[14] by conducting a SQL injection attack against a Southwest United States CAD network. Both attacker IP addresses were internal, likely indicating a prior compromise to an adjacent municipal network.

Credential abuse

A PSTA-led review of MITRE ATT&CK TTPs used in attacks against public safety (and employed by CTAs known to attack public safety) found that valid accounts and other credential abuse techniques were among the most commonly employed in successful and attempted cyberattacks. PSTA has observed CTAs using valid accounts to elevate privileges and log into remote systems, accessing mission-critical networks through services such as VPNs or through protocols like Windows Remote Desktop Protocol (RDP).

In one case in December 2024, an unnamed third-party vendor conducted a network switch upgrade for a U.S. county sheriff's office, however an error resulted in the servers being exposed to the internet. A CTA identified one of the exposed servers and attempted to brute force the login over the secure shell (SSH) protocol. Endpoint detection and response (EDR) solutions installed on the network helped identify and block the attempt.

Targeting remote services

Remote access tools, particularly free-to-use solutions, are appealing to CTAs as they can provide streamlined access to victim systems. The MS-ISAC CIRT investigated two incidents impacting public safety entities in 2024 where CTAs appeared to gain initial access to victim systems leveraging poorly managed VPN appliances. In the first incident, the impacted entity received an alert from Windows Defender and saw Cobalt Strike activity. They also noticed brute force activity against admin accounts and saw a successful compromise of a domain administrator account followed by the CTA disabling Windows Defender with group policy. In the second incident, CTAs

[13] https://nvd.nist.gov/vuln/detail/cve-2020-1472
[14] https://nvd.nist.gov/vuln/detail/CVE-2025-1094

likely gained access to a county network through an unpatched VPN solution. The CTAs then pivoted from the county network to infect a sheriff's office with ransomware.

Similarly, PSTA observed an incident where the Hunters International ransomware group leveraged compromised credentials to log into an unsecured VPN connection to access a large county's IT network in March 2024. The group used RDP and compromised a domain administrator account to move laterally across the network. Over 800 workstations and a central dispatch system were encrypted, resulting in defenders taking 96 hours to reach full containment before remediation efforts could begin.

Phishing & social engineering

Google's M-Trends 2025 report found that email-based phishing featured as the third most frequent initial access vector, comprising 14% of total detections.[15] In August 2024, PSTA identified that CTAs had used a phishing email to compromise a city mayor's personal Gmail account, which enabled the CTAs to pivot to the city's enterprise IT system. CTAs then moved laterally, deploying ransomware across the entire municipal IT environment and the county CAD system. The attack forced police officers and dispatchers to use "paper and walkie-talkies" to share critical dispatch information.

Malware (SocGholish)

The top three malware the MS-ISAC observed impacting public safety entities in 2024 were SocGholish, Magecart, and XCodeGhost. SocGholish was overwhelmingly the most common malware impacting the sector, comprising 92% of malware detections. SocGholish is a downloader written in JavaScript that is distributed through malicious or compromised websites via fake browser updates. The malware uses multiple methods for traffic redirection and payload delivery, commonly uses Cobalt Strike, and steals information from the victim's system. Additionally, SocGholish can lead to further exploitation, such as by loading NetSupport and Async remote access tools or even ransomware in some cases.

In February 2025, defenders identified and blocked an attempted Domain Name Service (DNS) lookup associated with SocGholish malware on a public safety entity's CAD system. PSTA analysts assessed this was caused by a user operating a CAD workstation enabled with email clicking a phishing link or navigating to a CTA-controlled domain. This would have initiated the chain of JavaScript requests leading to payload installation and detonation of SocGholish. Both PSTA and the MS-ISAC CTI team released written products on related SocGholish activity in March and early April 2025.

[15] https://cloud.google.com/blog/products/identity-security/from-insight-to-action-m-trends-agentic-ai-and-how-were-boosting-defenders-at-rsac-2025

Distinct challenges for public safety

Public safety mission-critical networks support technologies with extremely high availability requirements. Additionally, the prevalence of legacy systems makes it difficult to implement proper controls and adequately monitor environments using managed detection and response (MDR) solutions not tailored to public safety systems. PSTA engagements have revealed these systems often feature security issues like high levels of shared accounts, failure to manage appropriate user permissions and system accounts, and incoming and outgoing connections through unsecured VPNs and protocols like RDP. An additional challenge is that many public safety technologies are either directly connected or reliant on municipal and law enforcement networks. If not properly configured, segmented and secured, this network structure presents significant opportunities for CTAs with access to enterprise IT environments to move laterally and access mission-critical systems.

Additionally, CTAs with access to backbone network infrastructure under these conditions pose a significant threat to the availability of connected systems. Attackers encrypting enterprise systems, even without directly accessing mission-critical networks, can still disrupt those functions in specific circumstances.

Data sensitivity

Public safety entities house and administer highly sensitive data. They frequently maintain databases including case information containing personally identifiable information (PII) on suspects, victims, witnesses, persons of interest, vulnerable individuals, staff, family members, and more. Many of these data types are subject to compliance laws including Criminal Justice Information Services (CJIS)[16] and others. In 2024, PSTA observed 28 credible offers on cybercrime forums advertising data harvested from public safety networks. These offers were in addition to exfiltrated data stemming from ransomware attacks where CTAs leveraged stolen law enforcement and municipal data to further extort victims and malware with infostealer capabilities like SocGholish.

When departments suffer data breaches, CTAs leaking data have posed additional threats to impacted individuals resulting in doxxing, identity theft, swatting, and more. In one example in June 2024, the BlackSuit ransomware group uploaded data belonging to a major city's Police Department on their data leak website after the group failed to receive the ransom payment from a May 2024 attack. The leaked information included crime scene photos, evidence and records, and officer information.

[16] https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center

Sector cyber maturity comparison

The Center for Internet Security (CIS) released the latest edition of its Nationwide Cybersecurity Review (NCSR) in early April 2025.[17] The NCSR is a no-cost, anonymous, annual self-assessment for SLTT entities broken down by sector. The NCSR scores agencies' cyber maturity based on five NIST Cybersecurity Framework (CSF) Functions,[18] labeled: Identify, Protect, Detect, Respond, and Recover. Scores range from 1-7. The lowest score, labeled "Not Performed," means organizations have not begun implementing these policies. The highest score is labeled "Optimized," meaning organizations have executed, documented, tested, verified, and reviewed policies to ensure continued effectiveness. Despite limitations in implementing cybersecurity best practices across the attack surface, both state and local public safety and law enforcement agencies scored favorably across functions relative to their peer groups, averaging 4.59 across all functions, or "Partially Documented Standards and/or Procedures."

Public safety scores across functions were generally consistent, earning the lowest marks for "Identify - Risk Management Strategy" with an average score of 4.14.

MITRE ATT&CK patterns observed

IT systems:

- [T1059] — Execution
- [T1078] – Valid Accounts
- [TA0101] – Command and Control
- [T1110] – Brute Force
- [T1133] – External Remote Services
- [T1589] – Gather Victim Identity Information
- [T1189] – Drive-by Compromise
- [T1210] – Lateral Movement – Exploitation of Remote Services
- [T1219] – Remote Access Tools
- [T1562] – Impair Defenses: Disable or Modify Tools

[17] https://www.cisecurity.org/ms-isac/services/ncsr
[18] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

- [T1566] – Phishing
- [T1486] – Data Encrypted for Impact

Public safety mission-critical systems:

- [T1595] — Active Scanning
- [T1566] — Phishing
- [T1190] — Exploit Public-facing Application
- [T1133] — External Remote Services
- [T1078] — Valid Accounts
- [T1078.002] — Domain Accounts
- [T1110] — Brute Force
- [T1110.003] — Password Spraying
- [T1021] — Remote Services
- [T1021.001] — Remote Desktop Protocol (RDP)
- [T1657] — Financial Theft
- [T1486] — Data Encrypted for Impact

Analytic confidence

Analytic confidence in this assessment is moderate to high. Source reliability is high but is limited by incomplete data points, particularly concerning incident data. Time was one month to research this topic and the topic itself was not overly complex. The analysts' expertise includes cybersecurity and public safety-specific sector knowledge. The analysts worked as a small group across teams to complete this product.

For questions or comments, please contact the MS-ISAC at intel@cisecurity.org and PSTA at psta@motorolasolutions.com. For further information on our analytic tradecraft, please refer to MS-ISAC's blog post[19] outlining these standards.

[19] https://www.cisecurity.org/ms-isac/services/words-of-estimative-probability-analytic-confidences-and-structured-analytic-techniques

Recommendations

To better defend against maturing threats against the sector, public safety entities should implement the following recommendations, focusing principally on asset inventory, securing and segmenting remote systems and critical communication technologies. Agencies should also strive to enhance processes to level five NCSR maturity, which the report describes as: "Your organization has an activity or process defined within documented policies, standards, and/or procedures" and "[y]our organization is in the process of implementing and aligning the documentation to a formal security framework and/or methodology." Numerous departments have undertaken proactive efforts to enhance their security policies and crisis preparedness. In one example, Fairfax County, Virginia 9-1-1 and Metro Nashville Davidson County, Tennessee partnered to implement a network interoperability system[20] to provide backup support during a local or regional outage.

Beyond these efforts, departments should implement and consult the following guidance and resources to better secure mission-critical communication technologies and IT systems.

Motorola Solutions PSTA guidance

Recommendations are largely adapted from applicable U.S. Cybersecurity and Infrastructure Security Agency (CISA) Cross-Sector Cybersecurity Performance Goals.[21]

- Employ multi-factor authentication (MFA). All IT accounts should leverage MFA to access organizational resources. Defenders should prioritize accounts with the highest risk, such as privileged administrative accounts with access to mission-critical systems.
- Patch known vulnerabilities. All known exploited vulnerabilities in internet-facing systems ought to be patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first and flaws which allow for remote code execution (RCE).
- Change default passwords. Enforce an organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware related to mission-critical systems before putting on any internal or external network.
- Employ network segmentation. All connections to mission-critical networks should be denied by default unless explicitly allowed for specific system functionality. Necessary communications paths between IT and mission-critical networks must pass through an intermediary, such as a properly configured firewall, bastion host, or a demilitarized zone, which is closely monitored and only allows connections from approved assets.
- Limit mission-critical connections to the open internet. No mission-critical assets should be on the public internet, unless explicitly required for operation. Exceptions must be justified

[20] https://www.fairfaxcounty.gov/news/county-9-1-1-launches-first-interstate-backup-system-united-states
[21] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (e.g., MFA, mandatory access via proxy).

- Leverage MDR.[22] Suspicious activity, such as failed logins, unusual network traffic, use of tools like PowerShell, and activation of command line interfaces should be logged and sent to 24/7 monitoring teams such as an organization's dedicated security operations center or to third party experts. Where possible, automated solutions should be implemented to reduce defender workloads and decrease time until potential threat remediation

MS-ISAC guidance

- Implement the CIS Critical Security Controls[23]
    - The CIS Critical Security Controls (CIS Controls) are a prescriptive, prioritized, and simplified set of best practices that organizations can leverage to strengthen their cybersecurity posture.
    - Organizations looking for a place to start should focus on Implementation Group (IG) 1, which CIS defines as "essential cyber hygiene."[24]
- CIS Endpoint Security Service (ESS) can help mitigate malicious file execution by blocking unauthorized activities at the endpoint (i.e., host, server).[25]
- Malicious Domain Blocking and Reporting (MDBR) is an MS-ISAC member service that proactively blocks an organization's DNS traffic from connecting to known harmful web domains. Additionally, MDBR+ is a cost-effective offering that builds on the existing capabilities of MDBR and provides SLTT organizations with a quick-to-configure and easy-to-deploy, cloud-based secure web gateway service that enables them to further reduce risk and increase their security defenses.[26]
- Network Intrusion Detection System (NIDS):[27] Albert is a NIDS available to SLTT governments. Albert utilizes a unique signature set specifically developed for SLTTs to ensure sensors rapidly recognize and alert on potentially malicious traffic occurring on the network.
- CIS Passive Monitoring Services[28] leverage the MS-ISAC SOC to alert enrolled SLTT members after identifying CTA claimed access to sensitive resources including valid credentials, initial access offerings, and malicious domain and IP compromises.

---

[22] https://www.motorolasolutions.com/en_us/managed-support-services/cybersecurity/activeeye-security-platform.html
[23] https://www.cisecurity.org/controls/cis-controls-list
[24] https://www.cisecurity.org/controls/implementation-groups/ig1
[25] https://www.cisecurity.org/services/endpoint-security-services
[26] https://www.akamai.com/blog/security/introducing-mdbr-customized-security-for-government-organizations
[27] https://www.cisecurity.org/services/albert-network-monitoring
[28] https://www.cisecurity.org/ms-isac/services

- Resources:
    - CIS Combatting Ransomware guide[29]
    - Phishing Guidance: Stopping the Attack Cycle at Phase One[30]
    - MS-ISAC Guide to DDoS Attacks[31]

Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722



Public Safety Threat Alliance (PSTA)
www.motorolasolutions.com/PSTA
psta@motorolasolutions.com

[29] https://www.cisecurity.org/insights/white-papers/combatting-ransomware
[30] https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one
[31] https://www.cisecurity.org/insights/white-papers/ms-isac-guide-to-ddos-attacks

Appendix A: Traffic light protocol for disclosure

As part of the PSTA, agencies and other members are encouraged to share their own cybersecurity threat experiences to improve the awareness and readiness of the overall group. Submitting agencies should stipulate the level of disclosure required for their submissions according to the PSTA Traffic Light Protocol (TLP), based upon the CISA Traffic Light Protocol guidance,[32] which helps all members submit and leverage insights while being respectful of the submitting agency's preferences.



RED: Restricted to the immediate PSTA participants only

- When should it be used? Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.
- How may it be shared? Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting.



GREEN: Restricted to the community

- When should it be used? Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.
- How may it be shared? Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.





AMBER: Restricted to participants' organizations

- When should it be used? Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
- How may it be shared? Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves. TLP: AMBER+STRICT Restricts sharing to the organization only.



CLEAR: Disclosure is not limited

- When should it be used? Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
- How may it be shared? Subject to standard copyright rules, TLP: CLEAR information may be distributed without restriction.

[32] https://www.first.org/tlp/