



PSTA

Public Safety ISAO



Finished Intelligence Report



# Public Safety Threat Report: 2024 Threat Landscape

**Disclosure Protocol:** GREEN: Restricted to the community

**Date of Publication:** 31 January 2025

The Public Safety Threat Alliance (PSTA) threat intelligence team actively monitors and evaluates the threats to public safety. In this report, we examine the top threats and developments impacting public safety throughout 2024. Our team used both open and closed sources as part of our investigation, including information from our ActiveEye Managed Detection and Response team, private and trusted vendors, and government reporting. We used numerous intelligence analytical techniques in the assessment of threat intelligence provided in this report.

## Key Points

- Cyberattacks to global emergency services fell **22%** in 2024, driven by reduced extortion and access broker activity.
- Cyber impacts to mission-critical networks became increasingly common; attacks disrupting public safety radio, dispatch systems, and 9-1-1 call handling rose **44%**.
- State-sponsored attacks to U.S. critical infrastructure increased **75%**, generated by rising geopolitical tensions.
- Zero-day exploitations are happening more frequently, with multiple public safety attackers targeting novel vulnerabilities.

## Executive Summary

The cyber threat landscape continues to evolve year after year. While global cyberattacks impacting public safety fell in 2024, disruptions to key mission-critical systems like land mobile radio, computer aided dispatch, and 9-1-1 call handling rose dramatically. Dispatch systems underwent an **89%** spike in cyber disruptions alone, driven by opportunistic attacks on enterprise networks but also an assessed preference and capability from threat actors to disable mission-critical technology to receive extortion payments.

Other forms of malicious cyber activity are also on the rise. Nation state-sponsored campaigns targeted critical infrastructure, and adversaries of multiple levels of technical sophistication increasingly used zero-day vulnerabilities when conducting attacks. The growing capability of cyber attackers through increased nation-state intervention and well financed criminal groups significantly escalates the required defensive posture of public safety organizations.

**TLP: GREEN**



**MOTOROLA SOLUTIONS**



PSTA

Public Safety ISAO



# Finished Intelligence Report



Tabletop exercises, comprehensive security monitoring, and participation in information sharing networks can all act as force multipliers to identify and thwart would-be attackers.

## Landscape Overview

Successful and validated cyberattacks globally to public safety organizations declined but became more impactful. Overall compromises decreased by **22%** compared to last year, totaling **292** incidents. However, successful attacks in 2024 were the most destructive ever, regularly shutting down essential mission-critical systems.

A decline in extortion and initial access broker (IAB) activity contributed to the overall fall in attacks. However, despite a **10%** drop, extortion with ransomware remained the most prevalent attack type (See Figure 1). A **36%** decrease in IAB postings for public safety agencies suggests brokers are shifting their focus on other sectors, as well as establishing exclusive partnerships with top extortion groups. This is evidenced by the continued growth in IAB activity on the dark web throughout 2024. Reduced stolen credential sales strongly contributed to the decline in emergency services impacts, as credential abuse continues to be the number one tactic for initial access for the second year in a row.

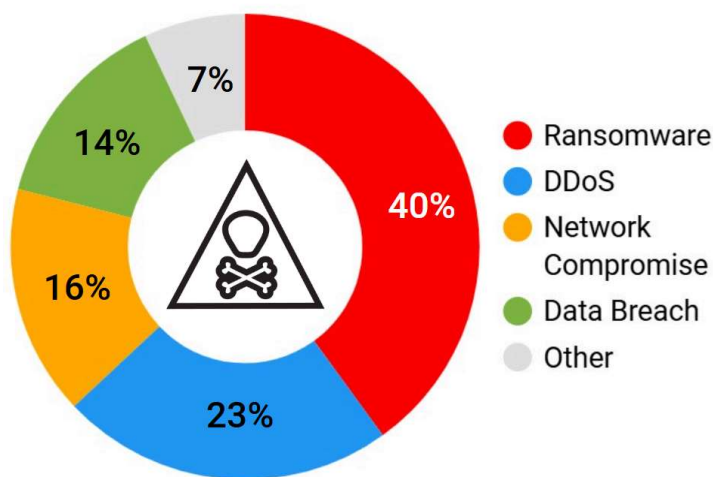


FIGURE 1: Types of attacks impacting public safety in 2024

Zero-day exploits became increasingly prominent in the 2024 threat landscape. According to the Joint Cybersecurity Advisory report, **73%** of the top 15 vulnerabilities listed on the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) Catalog<sup>1</sup> were initially exploited as zero-days<sup>2</sup>. Public safety attackers have found high success in 2024 focusing on these popular and new vulnerabilities. **26%** of the exploits used in public safety attacks in 2024 were among the top 10 most common exploits observed by CISA. Adversaries are expected to continue to leverage

<sup>1</sup> <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

<sup>2</sup>

<https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/article/3961769/cisa-nsa-and-partners-issue-annual-report-on-top-exploited-vulnerabilities/>

TLP: GREEN



MOTOROLA SOLUTIONS



PSTA

Public Safety ISAO



# Finished Intelligence Report



zero-day and recently announced vulnerabilities against public safety, as exploits become more available to purchase on criminal forums and access credentials are slightly declining in sales.

Hacktivism remained a persistent but low-impact threat to public safety agencies throughout the year. The vast majority involved distributed denial of service (DDoS) attacks, motivated by the ongoing war in Ukraine and escalating conflicts in the Middle East. However, **7%** of observed hacktivist attacks used ransomware and data breaches, suggesting growing sophistication of some groups. Despite this, an overall increase in higher-impact hacktivist attacks is unlikely, as most ideologically-motivated groups lack the sophistication, infrastructure, or financial means for such attacks.

## Rising Mission-Critical Attacks

Public safety radio, computer aided dispatch (CAD), and emergency call-handling systems are under regular attack for the first time on record. Disruptions to all aforementioned mission critical systems increased in 2024, with a total of **23** successful and validated cyberattacks causing partial or full disruption, up **44%** over last year. Most attacks involved ransomware and nearly all victims were located in the United States (See Figure 2). Compromises can have catastrophic consequences for first responders and the communities they serve, requiring a shift in how defenders approach the protection of mission-critical networks.



FIGURE 2: 2024 Cyberattacks impacting North American mission-critical networks

## Dispatch Operations

CAD environments were most commonly affected by cyberattacks in 2024, with **17** cyberattacks degrading services, an **89%** growth over 2023. Ransomware infections forced dispatchers to use pen and paper, rather than dedicated software and workstations. This made dispatching slower, more prone to error, and less interoperable with other mission-critical systems.

TLP: GREEN



MOTOROLA SOLUTIONS



PSTA

Public Safety ISAO



# Finished Intelligence Report



There are several assessed factors driving increased CAD disruptions (See Figure 3). First, extortion syndicates and their affiliates adopt the tactics of more successful groups — we saw this with the rise of double extortion.<sup>3</sup> In a ‘copycat’ situation, if one threat actor’s CAD disruptions seem to make ransom payouts more successful, other groups are likely to follow suit when striking public safety.

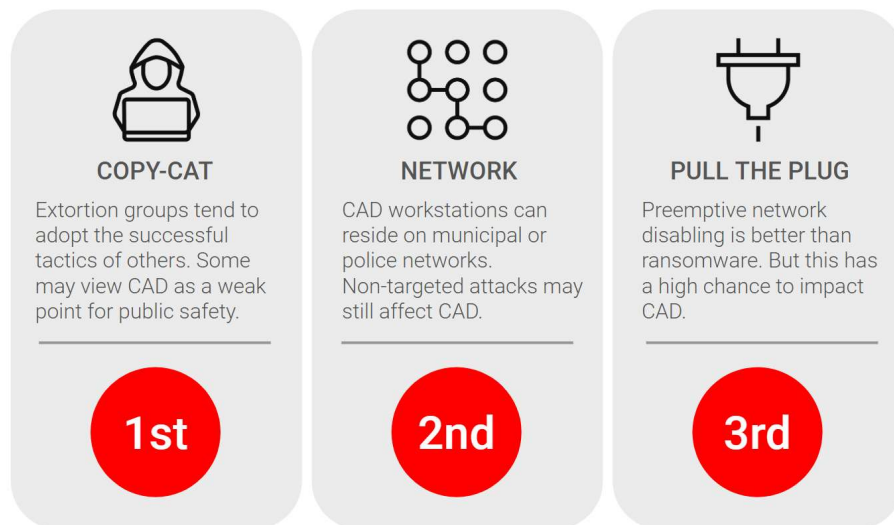


FIGURE 3: Likely factors influencing CAD disruptions in 2024

Second, CAD is the most easily accessed mission-critical system (when compared with LMR and 9-1-1 call handling). CAD workstations commonly reside on enterprise IT networks and dedicated connections to adjacent CAD server environments can provide direct access to critical systems when not properly managed. This means any opportunistic attack on a given public safety entity has a higher likelihood to affect dispatch systems than more isolated radio or next-generation call handling services.

Finally, defenders don’t always have an established plan or visibility into their networks to appropriately and effectively respond to a rapid cyber intrusion. Because CAD systems are more interconnected with enterprise IT networks, when defenders don’t have visibility into where a threat actor is hiding or a procedure to isolate the attack in a non-consequential manner, a growing number of victims are making the decision to disable the network entirely. This can also force ‘pen and paper’ operations on dispatchers. However, downtime to CAD systems is reduced to days or weeks, versus a month or more caused by a full ransomware detonation.

## Public Safety Radio

There were **four** cyber disruptions against broadband LTE and P25 radios, up from the **one** observed in 2023. Historically, cyber compromises against land mobile radio occur infrequently. Since 2018, nearly all malicious activity against LMR either involved criminal device thefts<sup>4</sup> or jamming attacks associated

<sup>3</sup> <https://gca.isa.org/blog/double-extortion-ransomware-what-it-is-and-how-to-respond>

<sup>4</sup> <https://www.cbc.ca/news/canada/toronto/toronto-police-tow-truck-radios-1.5622069>



MOTOROLA SOLUTIONS

TLP: GREEN





PSTA

Public Safety ISAO



# Finished Intelligence Report



with civil unrest or military actions. However, in 2024 disruptions forced radios offline, sometimes for weeks, showcasing the rising danger of mission-critical attacks.

LMR systems are secure by design, and the successful attacks in 2024 required misconfigurations and mismanagement to be successful. In two separate cases, adversaries scanning the open internet identified exposed virtual private networks (VPN) on the open internet with direct access to the core radio system. The VPNs had no multi-factor authentication or monitoring, and likely through password spraying techniques,<sup>5</sup> the attackers gained access to the P25 radio network to each county wide system. The attackers deployed ransomware, and in one instance inflicted weeks of downtime to the primary radio network. In that instance, defenders were forced to rely on a state-provided “communication on wheels” backup system while fully rebuilding the radio network.

## Emergency Call Handling

Cyberattacks impacting emergency call handling systems also rose in 2024 to a total of **five** validated disruptions, **four** involving ransomware. While attacks are still uncommon, the growing adoption of Next Generation 9-1-1 (NG911) can broaden the attack surface of public safety answering points (PSAPs) if not properly integrated and managed.

NG9-1-1 adoption continues to reduce the likelihood and impact of telephony-denial-of-service (TDoS)<sup>6</sup> attacks. We observed only **one** in 2024. On 04 August 2024, Central Texas 9-1-1 calls were rerouted to neighboring jurisdictions after a TDoS hit the Capital Area Council of Governments’ (CAPCOG) legacy 9-1-1 system. The attack caused “difficulty hearing callers and call-takers, [and] missing location information,” according to local reporting. At least 22 agencies, including the Austin Fire Department, were affected for approximately five hours.

## Advanced Persistent Threats

Nation state-affiliated adversaries are increasingly attacking critical infrastructure in the United States and abroad. This year, the PSTA observed **seven** separate campaigns impacting North American and U.S. critical infrastructure networks (See Figure 4), a **75%** increase over 2023. The top threat actors attacking critical infrastructure operated out of Russia, Iran, and China. Attributed groups like *VoltTyphoon*<sup>7</sup> maintained access to critical networks, likely to facilitate espionage and maintain strategic advantage.

<sup>5</sup> <https://attack.mitre.org/techniques/T1110/003/>

<sup>6</sup> [https://www.cisa.gov/sites/default/files/publications/Cyber%20Risks%20to%20911%20TDoS\\_6.4.2020%20-%20%28508c%29\\_0.pdf](https://www.cisa.gov/sites/default/files/publications/Cyber%20Risks%20to%20911%20TDoS_6.4.2020%20-%20%28508c%29_0.pdf)

<sup>7</sup> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>



MOTOROLA SOLUTIONS

TLP: GREEN

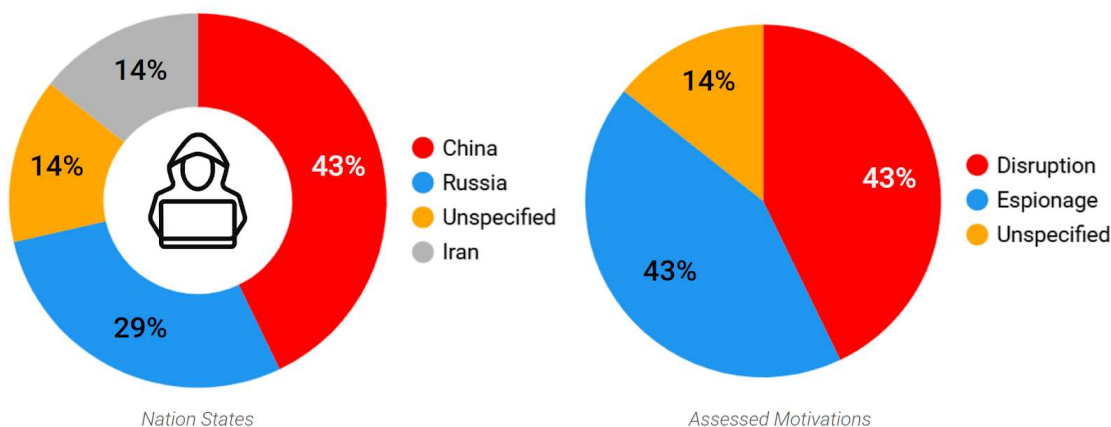


FIGURE 4: Observed state-sponsored campaigns impacting U.S. critical infrastructure in 2024

Worldwide APT activity continues to remain elevated, with countries like China focusing on strategic areas such as the Taiwan Strait. Nation-state cyber campaigns are typically driven by a desire to gain advantages in regional tensions and achieve strategic goals. From November 2023 to April 2024, security researchers observed the Chinese APT *RedJuliet* exploiting vulnerabilities against network edge devices,<sup>8</sup> with **86% (85 out of 99)** of cases involving Taiwanese entities, including government organizations. This campaign was designed to “support Beijing’s intelligence collection on Taiwan’s economic and diplomatic relations.”

The war in Ukraine also motivates continued Russian targeting of Western organizations. According to the 2024 Microsoft Digital Defense Report, “**75%** of [Russian APT] targets were in Ukraine or a NATO member state, as Moscow seeks to collect intelligence on the West’s policies.”<sup>9</sup>

## The Ransomware Connection

Some APT campaigns aimed to directly deploy ransomware on their targets or assist other threat actors in deploying ransomware to achieve their nations objectives. Cyber operatives from China, Iran, and North Korea were all observed communicating with or directing cybercriminal extortion groups. CISA detailed how Iranian adversaries targeted infrastructure, government, and energy networks, aiming to “obtain credentials and information describing the victim’s network that can then be sold to enable access to cybercriminals.” This is consistent with prior observed behavior in which Iranian APTs posed as financially-motivated access brokers to influence ransomware operations to target victims in line with Iranian state interests.

The growing connection between some APTs and extortion syndicates is part of a larger trend of cybercriminals cooperating with nation states. According to Microsoft, Russian APTs “outsourced some of their cyberespionage operations to criminal groups, especially operations targeting Ukraine.” In

<sup>8</sup> <https://www.recordedfuture.com/research/redjuliett-intensifies-taiwanese-cyber-espionage-via-network-perimeter>

<sup>9</sup> <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024>

a June 2024 instance, cybercriminals used commodity malware to attack roughly 50 Ukrainian military devices, which Microsoft indicates was at the behest of a Russian APT or state entity.

## Tradecraft & Tooling

### Top Techniques

Threat actors favored credential abuse tactics in 2024, with **46%** of public safety attackers leveraging stolen credentials in their operations. Adversaries leveraged valid accounts to gain initial access, move laterally, and maintain persistence by mimicking legitimate activity. Most notably, one such case facilitated an attack that disrupted radio communications. Compromised credentials were most frequently obtained from the dark web, brute force attacks, and phishing. Cybercriminals can use one or all of these methods interchangeably, as public safety attackers tend to be opportunistic, seeking to maximize their chances of success.

Threat actors exploited vulnerabilities in public-facing applications but relied more on zero-days. Notably, **37%** of public safety attackers began attacks via the exploitation of public-facing applications. Adversaries also frequently targeted vulnerabilities in platforms such as Citrix ADC and FortiOS. This demonstrates threat actors capitalizing on delayed remediation efforts and quickly acting on previously unknown vulnerabilities.

### Top Tools

Adversaries most frequently relied on a combination of native tools, legitimate software, and malware to conduct their attacks (See Figure 5). Nmap and Nmap were used to gather additional information either during the reconnaissance phase prior to attacks or within defender networks. PSEXec was commonly used to execute commands across compromised systems, enabling attackers to expand their foothold within target networks. The use of PSEXec also allowed attackers to remain undetected during this lateral movement phase.

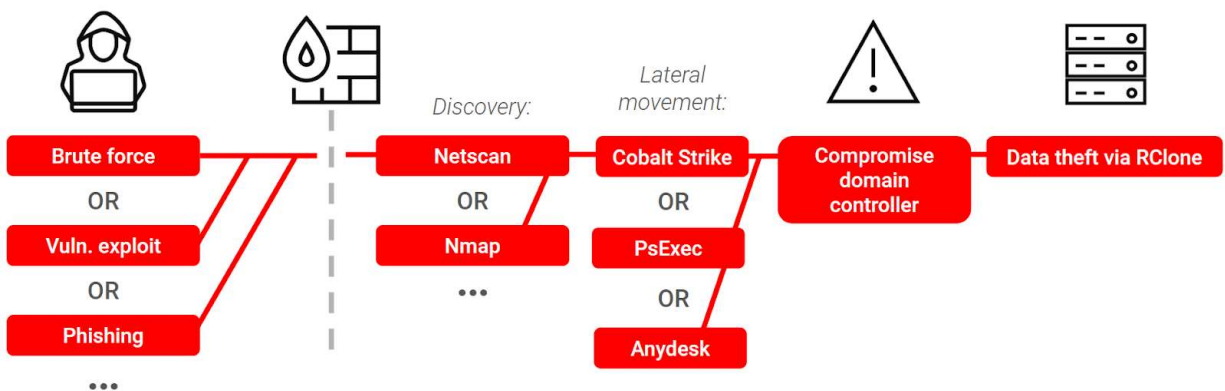


FIGURE 5: Example of how native tools and malware can be combined in an attack

Legitimate programs like PsExec were often combined with Cobalt Strike, a top tool for lateral movement and command and control (C2) operations. This integration of native tools and malware allowed the threat actors to evade detection and granted a range of options for achieving attack goals. Defenders are encouraged to continuously enhance monitoring capabilities by looking for unusual patterns of legitimate tool usage throughout environments.

## Mitigations

The 2024 threat landscape underscores the need for adaptive defense strategies as cyberattackers continue to increase their sophistication in their tradecraft and tools. It is important for defenders to respond to keep pace with the evolving threat landscape. Regularly maintaining cybersecurity hygiene along with best security practices is vital. However, defenders are encouraged to prioritize several practices heading into the new year (See Figure 6).



FIGURE 6: Top recommendations for public safety organizations

Public-facing applications and internal systems are more likely to be opportunistically targeted with recently disclosed or zero-day vulnerabilities. To minimize exposure to vulnerability exploitation attacks, defenders must maintain an up-to-date inventory of internet facing assets in their network. By keeping an inventory, security teams can run routine assessments and patch known vulnerabilities to minimize attack surfaces. Additionally, proper segmentation and access rules can halt attackers' progress, even after they gain access.

Implementing least privilege access policies, multi-factor authentication (MFA), and strict protocols over administrative tools can significantly reduce an attacker's ability to advance or escalate privileges once inside the network. Conducting tabletop exercises (TTXs) is an effective way to test whether optimal network segmentation and access controls have been properly implemented.

TTXs can also be extremely helpful in preparing defenders for inevitable cyber events. Adversaries have common playbooks for their attacks and defenders should as well — knowing where data backups are located, ensuring they are off-network, and practicing restoring disrupted systems is one way TTXs train for a real cyberattack. Defenders are recommended to review their incident response plans, test





PSTA

Public Safety ISAO



## Finished Intelligence Report



their ability to detect and mitigate the latest attack techniques, and identify any gaps in their defenses or communication protocols. Regularly conducting TTXs ensures that defenders can adapt to attack patterns and evolving threats targeting public safety.

Participating in an Information Sharing and Analysis Organization (ISAO) is a critical component of strengthening collective defenses for public safety organizations. This will enhance a public safety organization's security posture at no-cost through facilitating the exchange of threat intelligence and best practices. Organizations with long-term participation in an ISAC statistically demonstrate higher cybersecurity maturity levels compared to those with limited involvement, showcasing the critical role of information sharing.



**MOTOROLA** SOLUTIONS

TLP: GREEN







## Appendix A: Assessment and Response Standard Operating Procedures

### Levels of Analytic Confidence

High Confidence	Moderate Confidence	Low Confidence
Generally indicates judgments based on high-quality information, and/or the nature of the issue makes it possible to render a solid judgment. A "high confidence" judgment is not a fact or a certainty, however, and still carries a risk of being wrong.	Generally means credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence.	Generally means questionable or implausible information was used, the information is too fragmented or poorly corroborated to make solid analytic inferences, or significant concerns or problems with sources existed.

## Appendix B: 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](#), which helps all members submit and leverage insights while being respectful of the submitting agency's preferences.

 <p><b>RED:</b> Restricted to the immediate PSTA participants only</p> <ul style="list-style-type: none"> <li><b>When should it be used?</b> Sources may use <b>TLP: RED</b> 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.</li> <li><b>How may it be shared?</b> Recipients may not share <b>TLP: RED</b> 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, <b>TLP: RED</b> information is limited to those present at the meeting. In most circumstances, <b>TLP: RED</b> should be exchanged verbally or in person.</li> </ul>	 <p><b>GREEN:</b> Restricted to the community</p> <ul style="list-style-type: none"> <li><b>When should it be used?</b> Sources may use <b>TLP: GREEN</b> when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</li> <li><b>How may it be shared?</b> Recipients may share <b>TLP: GREEN</b> 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. <b>TLP: GREEN</b> information may not be released outside of the community.</li> </ul>
 <p><b>AMBER:</b> Restricted to participants' organizations</p> <ul style="list-style-type: none"> <li><b>When should it be used?</b> Sources may use <b>TLP: AMBER</b> when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</li> <li><b>How may it be shared?</b> Recipients may only share <b>TLP: AMBER</b> information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. <b>TLP: AMBER+STRICT</b> Restricts sharing to the organization only.</li> </ul>	 <p><b>CLEAR:</b> Disclosure is not limited</p> <ul style="list-style-type: none"> <li><b>When should it be used?</b> Sources may use <b>TLP: CLEAR</b> when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</li> <li><b>How may it be shared?</b> Subject to standard copyright rules, <b>TLP: CLEAR</b> information may be distributed without restriction.</li> </ul>