White Paper

CISA Land Mobile Radio best practices

Protect your ASTRO system from cyber threats

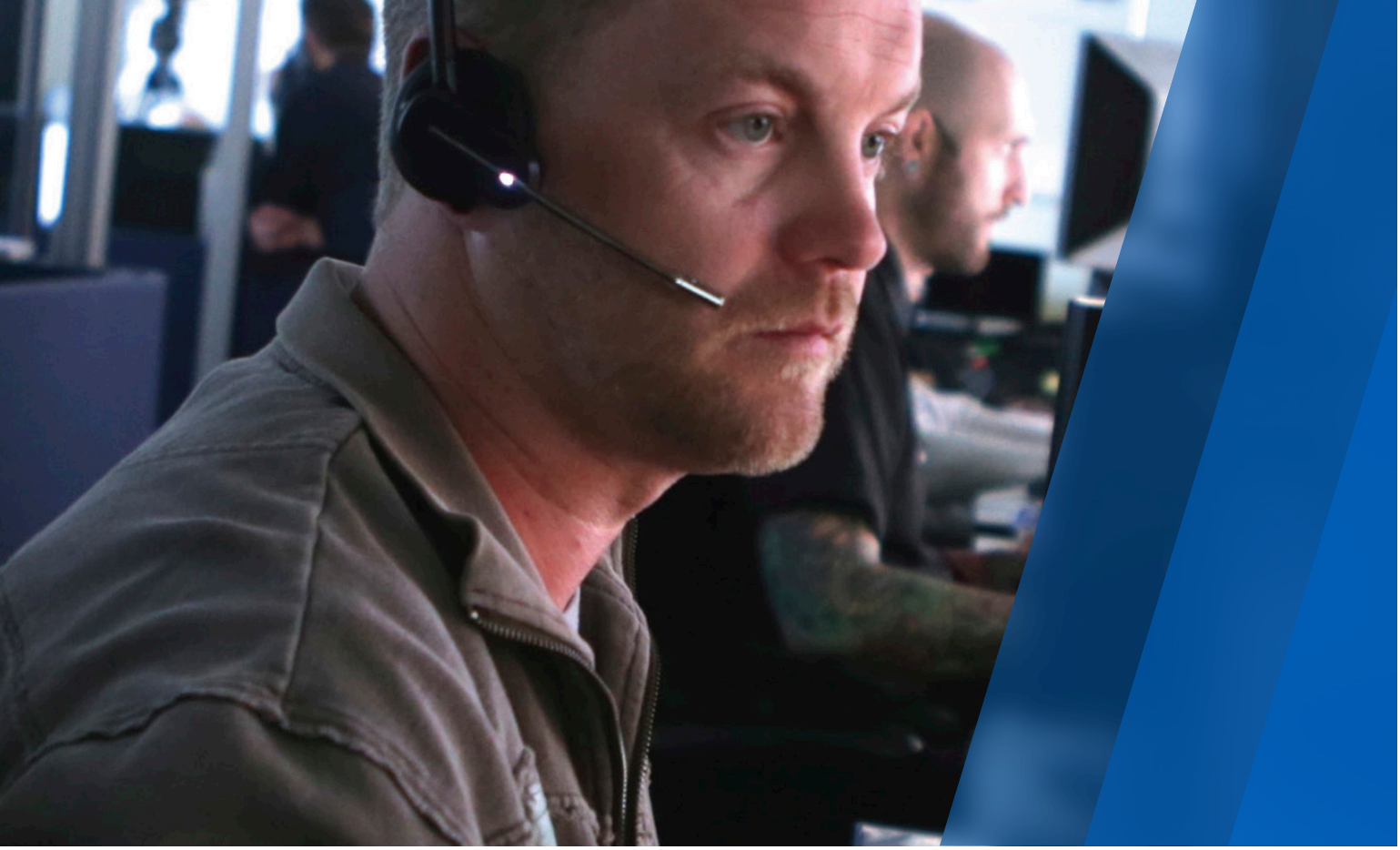
MOTOROLA SOLUTIONS

Confidently adopt innovations and defend LMR systems from cyber attacks

In this white paper, we outline six key steps for adopting innovations and reducing the risk of system downtime based on cybersecurity best practices.

The U.S government's Computer and Information Security Agency (CISA) regularly issues advisories outlining how cybersecurity-related risks have the potential to impact the availability, integrity and confidentiality of Land Mobile Radio (LMR) systems. Applying proper controls can mitigate LMR risks and increase system availability. Proactively planning for threats can decrease system downtime from cyber attacks or potentially avoid them altogether. This white paper recommends best practices for implementing the guidance in the CISA Cyber Risks to Land Mobile Radios report.

Why is this more of an issue now? Modern LMR systems are increasingly complex, with interconnections between LMR systems and broadband networks. These interconnections, while necessary, can introduce opportunities for exploitation if they are not properly configured. Additionally, while useful new features and data-driven insights enable first responders, they also introduce more software that threat actors can exploit if not properly updated. However, these new features are safe to adopt as long as proper security assessments and monitoring are in place.



Six key steps

Step 1: Acknowledge that LMR systems are susceptible to vulnerabilities and attacks.

As such, assess the LMR system network components/security posture and understand the various forms of cyber threats that can impact them.

Best Practice Guidance for LMR

- If you would like more visibility into the impact of cyber threats on public safety systems, join the Public Safety Threat Alliance (PSTA). The PSTA is a cyber threat Information Sharing and Analysis Organization (ISAO) that provides the public safety community with actionable intelligence that aids them in defending against cyber attacks. Membership in the PSTA is no-cost and provides you with access to finished intelligence reports created by the PSTA threat intelligence team.

To learn more, visit:

motorolasolutions.com/PTSA

Step 2: Develop and implement cyber incident and vulnerability response plans.

Your incident response (IR) plan should establish the policies and procedures to provide identification, evaluation, remediation, reporting and notification of incidents and vulnerabilities impacting systems, data and networks.

Best Practice Guidance for LMR

- The organization should have a cybersecurity Incident Response Plan that covers threats to information technology (IT) and operational technology (OT) systems found within LMR, such as:
  - Transmission interference or jamming
  - Interception or eavesdropping of conversations
  - Weak network remote access practices or loss of credentials
  - Physical intrusions or environmental events leading to component loss or disruption
  - Lost or stolen subscriber devices
- Identify responsible stakeholders, including internal staff and vendors, and their methods of contact. For an LMR system, both the system technicians and system owner should be identified as key points of contact.
- Base all preparation, detection and analysis, containment, eradication and recovery processes (and related courses of action) on sound risk assessment/management principles and the organization's risk tolerance/appetite, among others. The ASTRO system, like other public safety systems, should be considered a critical system.
- Develop and document plans for backup methods of communication (ex: Limited or Site trunking mode for radio systems).
- Build an accompanying strategic communications plan (or annex to the IR Plan) so the organization can provide synchronized/consistent IR and service disruption/outage messaging to key stakeholders, constituents and the general public.
- Consider any requirements imposed by legal or regulatory frameworks such as Criminal Justice Information Service (CJIS).
- Ensure the organization reviews the plan annually and tests the plan every two years.

For assistance with these best practices, see Motorola Solutions **Incident Response Planning**

Step 3: Implement regular security patching and updates.

It's important to keep operating systems and software up to date to address any known vulnerabilities in physical and virtual assets. Remove any unauthorized or outdated components from the system that could provide insecure access to the LMR network. Maintain proper encryption protocols and key management policies.

Best Practice Guidance for LMR

- As with any vendor, follow the recommended patch and update cycles in accordance with your organization's risk profile. In the case of Motorola Solutions, Motorola Technical Notifications (MTN) are published with critical update instructions that should be followed immediately. ASTRO customers should follow our Security Update Service's published patching cycle for the ASTRO system.
- In ASTRO, tested Windows patches are usually released on a monthly basis via Security Update Service (SUS), and critical-level patches should be installed soon after their release. Other Windows supported third party software patches should be installed after Motorola's careful testing, approval and publication.
- Windows systems in the ASTRO Radio Network Infrastructure (RNI) MUST be rebooted after installing patches. This reboot requires coordination among the users of the system. This can be challenging, but failure to reboot results in unapplied patches and will prevent patching on the next Motorola Solutions' release cycle.
- Patching servers in the Zone Core may require rollover of the active zone controller. This rollover may be disruptive to your dispatch operators, and should be coordinated. As an example, a Zone Controller rollover will cause a brief disconnection of any related consoles and should be coordinated with those users as well as any other teams involved in maintaining the system.

For assistance with these best practices, see:

Motorola Solutions **Security Update Service, Remote Security Update Service and Reboot Service**

Step 4: Regularly scan the network for abnormal activities.

Organizations should also develop security violation detection processes that the system users and administrators follow.

Best Practice Guidance for LMR

- Perform monthly scanning of the external interfaces of the radio network and dispatch sites with a focus on identifying configuration changes or new software vulnerabilities.
- Perform monthly scanning of the RNI with a focus on identifying newly added devices or unexpected open ports.
- Adjust scanning configurations against zone controllers and other critical components to maintain communications availability and integrity.
- Use a Dynamic System Resilience (DSR) core, if available, for penetration testing that may impact availability of the system.
- Leverage network intrusion detection and protocol analysis to evaluate RNI and primary CEN traffic flows for abnormal flows.
- Review system administration and remote access logs for abnormal activity.

For assistance with these best practices, see:

Motorola Solutions **Risk Assessments and Penetration Testing**

Step 5: Respond to cyber attacks immediately.

Immediate response can help reduce impacts on the system. Threats can be mitigated by having a well-developed incident response and disaster recovery plan that prioritizes resources.

Best Practice Guidance for LMR

- Implement Endpoint Detection and Response (EDR) on Radio Network Infrastructure (RNI) core systems, dispatch consoles and any endpoints in the Customer Enterprise Networks (CENs) to allow for rapid response actions.
- Implement network intrusion detection inside the RNI to identify any unapproved or malicious activity within the network.
- Monitor system logs and implement alerting on suspicious authentication, system activity and other sources of risk.
- Perform proactive threat hunting using all data sources with any new Indicators of Compromise (IOCs) or TTPs discovered to be targeting public safety through Public Safety Threat Alliance (PSTA) and other threat intelligence sources.

For assistance with these best practices, see:

Motorola Solutions **Managed Detection & Response Services**

Step 6: Get the LMR system back online as soon as possible.

Develop a comprehensive recovery plan that is periodically tested to ensure system users and technicians are prepared to respond to cyber attacks before they occur.

Best Practice Guidance for LMR

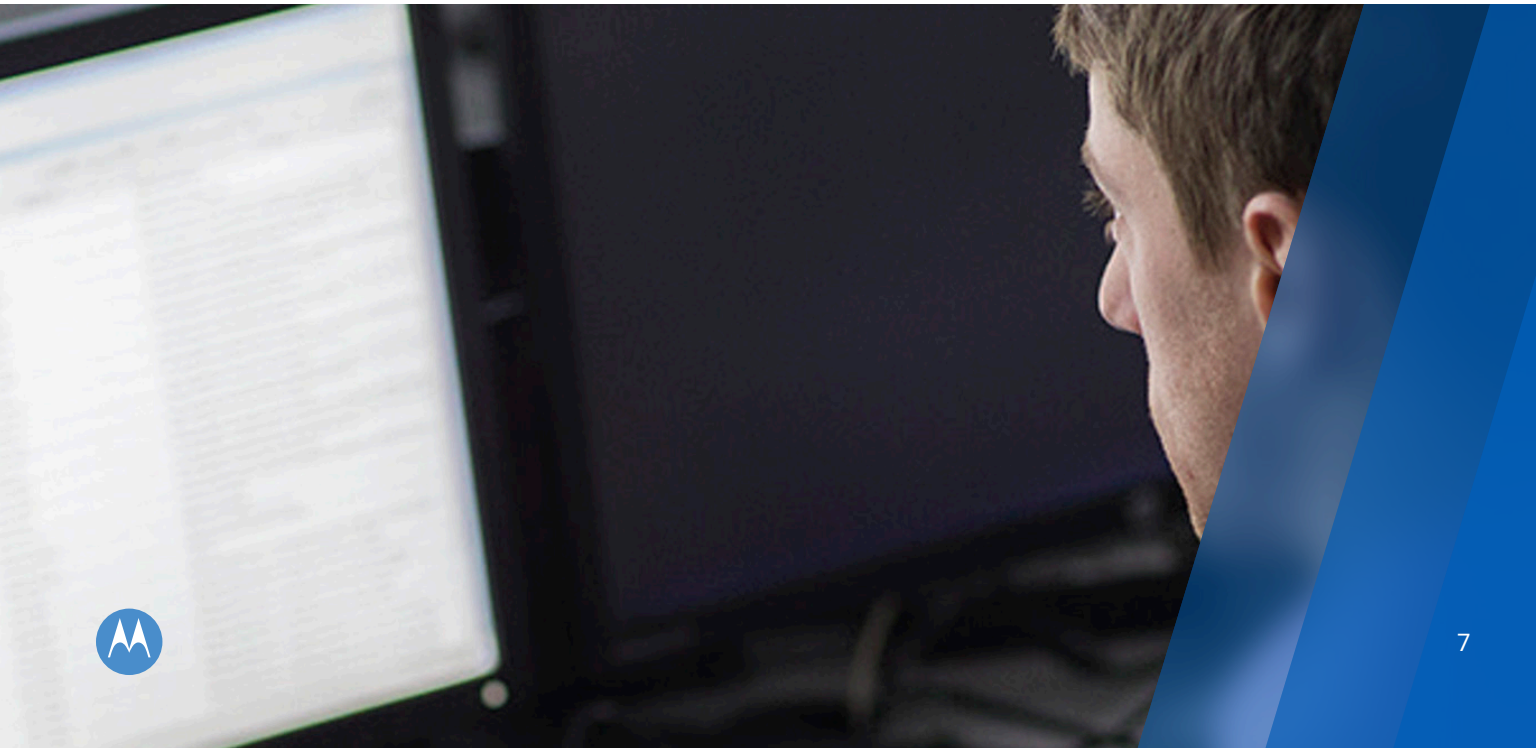
Ensure backups are successful on the Backup and Recovery (BAR) server. If recovery is required, notifications should be sent out to inform users that the system is down while restoration is in progress. A Business Continuity and Disaster Recovery (BC/DR) written plan should be in place that outlines:

- Stakeholders for business continuity/disaster recovery processes
- System criticality and business impact rankings
- Notification criteria
- Severity criteria to categorize the disaster
- Restoral time targets
- Communication plans
- Well-defined roles and responsibilities
- System specific plans for critical systems

Ensure your BC/DR as well as your cyber incident response plan are tested at least annually with critical stakeholders.

For assistance with these best practices, see:

Motorola Solutions **Advisory Services**



Maintain availability of your LMR system

Our Managed Detection and Response (MDR) and Advisory Services are customized for LMR to help ensure your system is resilient to cyber attacks.

- **Risk Assessment:**
  Our cybersecurity experts conduct deep and detailed ASTRO-based risk assessments that evaluate shared accounts, gaps in patching and updates. They also check for security best practices, such as network and user authentication. Assessments are composed of four parts: 1) interviews with the security and IT team 2) vulnerability scans 3) firewall configuration reviews 4) physical security assessments.

- **Incident Response (IR) Planning:**
  Our IR Planning services provide best-in-class training and exercises to ensure that when a security incident or attack happens, your organization will be prepared to handle it. Whether you want to minimize damages or you're concerned that you've been breached and don't know it, we're ready to help. Our proven agile and evidence-driven approach will keep you in control of whatever chaos an incident may bring.

- **Security Patching and Updates:**
  We work vigorously to identify, vet and test OEM Operating System and supported third-party security updates and patches that when applied pose a minimum impact to the operation and availability of the ASTRO system. Our rigorous testing methodology ensures functionality to include critical communications, application features and voice logging still work as designed post application of the updates and patches.

- **Managed Detection and Response:**
  Our MDR services monitor security infrastructure and systems 24/7 in the ASTRO Radio Network Infrastructure, as well as Customer Enterprise Networks (CENs) and IT networks. In addition, because we constantly monitor public safety networks, we are uniquely positioned to provide threat intelligence specific to them. This gives us deep insights to better protect against threats targeting these systems.

- **Incident Response and Recovery Planning:**
  Our IR planning team can create an incident management plan that is tailored to your organization's needs that outlines all of the critical functions necessary to identify, document and remediate a cybersecurity incident quickly. The IR plan will incorporate multiple stakeholders across your organization including legal, human resources, and emergency management.

- **Radio Authentication and Encryption:**
  One of the most important challenges ASTRO system managers face, and unfortunately one of the most common, is unauthorized radios that can't be verified before gaining access to the system. Whether a radio has been cloned, stolen, or simply lost, restricting network traffic to only authorized devices is critical. Our analysts can help you understand how to best use ASTRO system authentication and encryption tools to aid you in this effort.

  Equipped with AES-256 encryption and the Motorola Advanced Cryptographic Engine (MACE) chip, Motorola Solutions' APX radios protect your critical communication and the integrity of your operation. Validated at FIPS 140-3 Level 3, your voice and data communications are protected from misuse and illicit activity.

Maintain system availability with Managed Detection and Response (MDR)

Managed detection and response

- Powered by our ActiveEye platform.
- Deliver 24/7 threat management and data protection across networks, endpoints, cloud infrastructure and applications, plus mission-critical systems like ASTRO, VESTA 9-1-1 and CAD.
- Dedicated team of analysts provides actionable recommendations to prevent incidents, minimize risk and ensure best practices.

Security patching

- Patch identification to identify and fix weaknesses in your mission-critical systems. Includes testing and flexible deployment, both remotely and on-site.

Risk assessments and other professional services

- Penetration Testing
- Vulnerability Assessments
- Incident Response Planning
- Tabletop Exercises

Cybersecurity training

- We provide your employees with the means to develop their existing skills and learn new ones, ensuring that their knowledge is current and they remain confident in addressing cyber attacks.

To learn more, visit: **motorolasolutions.com/cybersecurity**

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2024 Motorola Solutions, Inc. All rights reserved. 08-2024 [RH04]