# Cyber Risks to Land Mobile Radio

## First Edition

Publication: 2022
Cybersecurity and Infrastructure Security Agency

# Cyber Risks to Land Mobile Radio

*First Edition*

## Overview

Land Mobile Radio (LMR) systems are designed to provide instant, reliable, and secure critical push-to-talk communications to the public safety and first responder community. However, the evolution of LMR systems from analog to digital has made these networks, devices, and data susceptible to cyber threats. Cyber risks manifest when a cyber attacker gains unauthorized access to a network, device, or data and affects the confidentiality, integrity, or availability of the system or information.[1] Some consider LMR networks closed systems that are not exposed to cyberattacks and do not see cybersecurity as an important component of their LMR system. However, LMR systems are vulnerable to multiple cyber risks that could negatively affect critical communications. This whitepaper provides an overview of LMR systems, explores various forms of cyber risks to public safety communications, and identifies methods and resources to help secure systems.[2] Additional addendums of this document are forthcoming as SAFECOM plans to develop content and resources focused on risks specific to analog LMR systems.

### How to Use this Document

This document is intended for public safety operations managers and agency officials to initiate vulnerability discussions with system owners and designers. They can use this document to familiarize themselves with:

- LMR systems and functions
- Cyber and physical risks to LMR systems
- Best practices and recommendations to mitigate cyber threats to public safety communications

Additional LMR and cybersecurity resources can be found in Appendix A. The checklist for all recommended steps can be found in Appendix B.

## Background

LMR systems are terrestrially based, wireless communications systems commonly used by federal, state, local, tribal, and territorial public safety, first responders, public works, commercial companies, and the military in tactical and non-tactical environments.

Supporting voice and low-speed data communications, LMR systems typically consist of handheld portable radios, in-vehicle mobile radios, control stations, base stations, and repeaters. A network ties the components together.

- **Handheld portable radios** are carried by operations personnel and tend to have a limited transmission range
- **Mobile radios** are often located in vehicles and use the vehicle's power supply and a larger antenna, providing a greater transmission range than handheld portable radios

[1] Cybersecurity and Infrastructure Security Agency (CISA), "Security Tip (ST04-001) What is Cybersecurity?" last modified November 14, 2019. https://us-cert.cisa.gov/ncas/tips/ST04-001.
[2] This document presents the most common LMR cybersecurity risks and provides planning and mitigation best practices. For additional guidance dedicated to LMR, see cisa.gov/publication/lmr-and-broadband-evolution. For Project 25 resources see https://www.cisa.gov/safecom/p25.

- **Base station radios** are in fixed locations, such as emergency communication centers (ECCs), public safety answering points (PSAPs), or dispatch centers, and tend to have the most powerful transmitters. They are essentially mobile radios that have been outfitted to operate as fixed infrastructure supplying a dispatch or control point for the system.
- **Repeaters** increase the effective communications range of handheld portable radios, mobile radios, and base station radios by retransmitting received radio signals
- **The network** connects LMR system components, serves as a transport mechanism for voice and data communications, and extends the communications coverage area of the LMR system. In addition to the LMR system components, LMR networks contain servers, routers, microwave systems, and in some cases, interface with private enterprise and/or public IP networks to increase the reach or coverage of the communications system and support interoperability

## Cyber Risks to LMR Systems

There are those who may perceive LMR systems to be analog or separate from other systems directly connected to the internet. However, the Confidentiality, Integrity, and Availability information security triad (CIA triad)[3] applies to LMR networks, devices, and data because the information being transmitted is sensitive and critical to public safety operations. Thus, LMR systems are a vector for malicious cyber actors to target public safety organizations. LMR systems are vulnerable to compromises such as unauthorized monitoring, eavesdropping, encryption hacks, disruptions of the physical infrastructure, and jamming of frequencies.

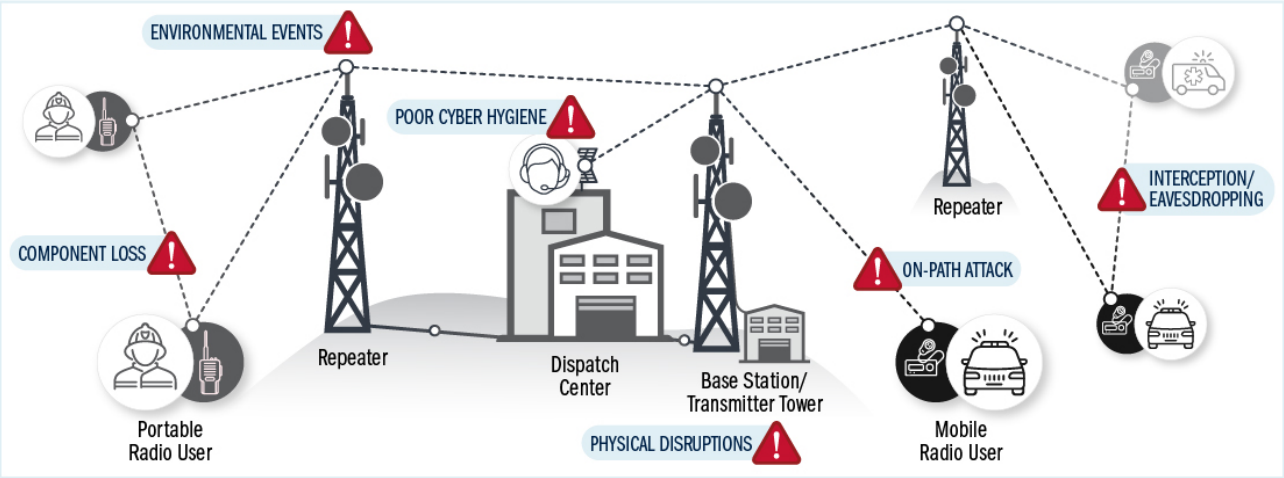


**Figure 1:** Examples of Cyber and Physical Risks within an LMR System

Many agencies are also implementing emerging wireless broadband services and applications. When broadband applications are enabled to support mission-critical voice applications, many public safety agencies may migrate to broadband voice applications to augment voice LMR systems to form a "converged network." For this document, a converged network is a dedicated, public safety wireless broadband infrastructure that offers mission-critical services, including voice, data, and video. The converged network could comprise cellular services and application-assisted integrated services required

[3] The CIA triad is a model where the principles of confidentiality, integrity, and availability guide an organization's information security policies and procedures. For more, see the National Institute of Standards and Technology (NIST) Special Publication 800-53 *Security and Privacy Controls for Information Systems and Organizations* https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

to connect LMR and cellular broadband users. The increase in interoperability and flow of data streams in the broadband and converged networks increases cyber risks to LMR systems.

**Figure 1** depicts potential physical and cyber risks related to the LMR system. This illustration is non-comprehensive, and the risks identified may occur at a variety of locations throughout the infrastructure. For risk definitions and additional examples, see **Table 1** on page 3, which lists and briefly describes cyber and physical risks facing LMR systems.

**Table 1:** Cyber Risks Facing LMR Systems

| Risk | Description |
|---|---|
| **Physical Risks** | |
| **Component loss** | The loss of LMR components (e.g., handheld radio) due to unintentional error or an intentional, malicious attempt |
| **Physical disruptions** | Attacks or alterations of the physical LMR equipment (e.g., RF towers, microwave dishes, and antennas) and sites |
| **Environmental events** | Unique, geographic region-based events that may physically harm the system (e.g., flooding, earthquakes, ice storms, tornadoes) |
| **Cyber Risks** | |
| **Radio frequency (RF) interference or "jamming"** | Unintentional or malicious disruption of RF to prevent wireless, cellular, broadband, or LMR communications |
| **Interception/eavesdropping** | Scanners and smartphone or web-based applications enable the public and those with criminal intent to listen to public safety transmissions and potentially acquire key response information |
| **Duplicate radio IDs** | In a trunked radio system, cybercriminals or rogue users could duplicate radio IDs and gain access to the system to disrupt communications |
| **Poor cyber hygiene** | Poor cyber hygiene—such as missing authentication/authorization, unpatched/ outdated software, and poor password management/policy—increases the risk of cyberattacks |
| **Unauthorized network access** | Poor encryption key management (e.g., compromised/outdated encryption keys), bypass of authorized methods and procedures, lost or stolen radios, and digital scanners or online applications being used to access communications |
| **Unauthorized data access** | Attackers can access sensitive databases (e.g., law enforcement, health records) to steal, modify, or corrupt data |
| **Denial-of-service attack** | Attackers flood the targeted host or network with traffic until the target cannot respond or crashes, leading to legitimate users being unable to access information systems, devices, or network resources |
| **On-path attack** | Wireless link between the user device and the RF site equipment may be susceptible and allow attackers to steal data or monitor conversations |
| **Insider threat** | Employees or other personnel with authorized or unauthorized access to the LMR network, devices, or data who knowingly or unknowingly affect the LMR system |
| **Malicious applications** | Attackers create apps that appear safe but allow them to steal, corrupt, or modify data |
| **Malware** | Files or programs (e.g., viruses, worms, trojans, spyware) that can harm a computer or compromise stored data |
| **Ransomware** | Malware that encrypts files until a ransom is paid or that exfiltrates data and then threatens to sell or leak it if the ransom is not paid |
| **Spearphishing** | A social engineering attack targeting specific individuals; the cybercriminals use email or malicious websites to solicit personal information by posing as a trustworthy organization; phishing attacks enable cybercriminals to gain initial access to LMR networks |

| Risk | Description |
|---|---|
| **Spoofing** | Unauthorized device masquerades as an authorized device to disrupt the network |
| **Supply chain attacks** | A supply chain attack occurs when a cyber actor gains access to a victim's system(s) and infiltrates the victim's supply chain partners (e.g., customers, suppliers) to gain access to their systems and data |
| **Hardware trojan** | Modifications made to firmware that may cause an interruption or undesirable effect on the function of the hardware |
| **Failure of synchronization** | Disrupting the system timing to delay call setup time, interrupt network transmitter sync, cause transmitter interference, and various latency between sites |
| **Disruption to trunked operations** | Disrupting or interfering with the control channel of a trunked radios system to deny service to users |

## Mitigating Cyber Risks

Maintaining secure and reliable communication modes is vital to the success of public safety missions. Cyber risks in LMR systems could result in loss of life or property, injuries, job disruption for affected network users, and financial costs associated with data misuse and subsequent resolution. Therefore, cybersecurity cannot be ignored or become an afterthought in the design, operation, and maintenance of LMR networks.

As described in **Table 1**, there are many vectors that malicious actors can use to gain access to LMR systems, causing loss of the confidentiality, integrity, or availability of the system. Mitigating these risks is the first step in ensuring the LMR system remains secure.

Public safety community members should use comprehensive cybersecurity best practices to plan for and mitigate cyber vulnerabilities and incidents. For example, the National Institute of Standards and Technology (NIST) recommends that public safety organizations routinely plan, prepare, and conduct drills for cyberattacks and incidents.[4] In addition, NIST recommends including responses to cyber incidents and system outages as an extension of the organization's contingency plan. The contingency plan suggests having incident response plans and procedures, trained staff, assigned roles and responsibilities, and incident communications plans established well in advance. It is recommended to periodically review and update the plan to ensure efficacy (e.g., on an annual basis, when there is a significant change in leadership, when new components are acquired and implemented).

NIST developed a cybersecurity framework to help critical infrastructure owners and operators identify and reduce risks. The framework comprises three parts: Framework Core, Framework Implementation Tiers, and Framework Profiles. Following such a framework can help system owners navigate the five phases of cyber risk management: Identify, Protect, Detect, Respond, and Recover[5].

### *Identify*

Gain a comprehensive understanding of the LMR system resources and their functions that pertain to the organization's cyber risks.

- **Identify what is on the network.** Inventory all hardware and software assets to distinguish what items could be vulnerable to cyberattacks. Establish a monitoring strategy to identify unusual

[4] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities Recommendations of the National Institute of Standards and Technology. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84. https://doi.org/10.6028/NIST.SP.800-84.
[5] Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, https://doi.org/10.6028/NIST.CSWP.04162018.

activity that could indicate an attack. The inventory process is not a one-time event. Policies and procedures must be in place to ensure the LMR system's inventory is monitored to ensure equipment remains in the organization's possession, is working properly, and has strong software/firmware versions, authentication and encryption keys.

## *Protect*

Institute strong safety mechanisms to ensure required services, features and functions are maintained.

- **Develop incident response and disaster recovery plans outlining roles and responsibilities.** Incident response plans and disaster recovery plans are crucial to LMR cybersecurity. Incident response plans mainly focus on information asset protection, while disaster recovery plans focus on operational continuity by minimizing recovery time for essential systems. Once the plans are developed, test them often using realistic simulations (e.g., "war-gaming"), assigning roles and responsibilities to the personnel who manage cyber incident responses. Testing ensures plans are effective and the appropriate personnel and stakeholders can effectively execute their responsibilities.[6]

- **Develop an internal reporting structure to detect, communicate, and contain attacks.** Effective communication plans focus on issues unique to security breaches. A standard reporting procedure will reduce confusion and conflicting information between leadership, the workforce, and stakeholders. Communication should be continuous, since cyberattacks could occur over a lengthy period. It should also come from top leadership or designated public information officers to demonstrate commitment to action and knowledge of the situation.

- **Keep all software, including operating systems, applications, and firmware, up to date.** Consider implementing a centralized patch management system. Enable automatic updates whenever possible. If feasible, obtain, test, and deploy the latest operating systems, applications, updates, and "patches" before installing them on a "live" system.

- **Implement secure configurations for all hardware and software assets so that both physical and virtual assets are protected.** Create and maintain policies that identify and prioritize secure configurations. Review and implement secure configuration guidance from vendors and other support sources. Conduct frequent vulnerability scans to identify and resolve weak or unprotected entry points.[7]

- **Remove unsupported or unauthorized hardware and software.** Inventory authorized hardware and software throughout the organization. Authorized hardware and software generally allow updates and patches to resolve potential system vulnerabilities. Know the physical location and user of the hardware to keep patching updates current. Identify and remove any hardware or software that is at the end-of-service-life and no longer supported with updates by vendors.

- **Create application integrity, allowlist, and blocklist policies so that only approved software can operate on the systems.** Ensure necessary applications perform in a secure and as-intended

[6] Review available incident response guidance, such as *the Public Power Cyber Incident Response Playbook* (https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf), a resource and guide to help organizations better organize around cyber incident response and to develop a cyber incident response plan.
[7] CISA offers a range of no-cost cyber hygiene services (https://www.cisa.gov/cyber-hygiene-services), including vulnerability scanning, to help critical infrastructure organizations assess, identify, and reduce their exposure to cyber threats, such as ransomware. By taking advantage of these services, organizations of any size will receive recommendations on ways to reduce their risk and mitigate attack vectors.

manner. Institute application integrity, allowlist, and blocklist control policies that allow only approved, authorized software and their libraries to load and execute programs. Monitor the integrity of allowlist applications with periodic checks of file hashes to ensure no unauthorized modifications have been made. Due to the complexity and effort required for identity and access management, consider a staged, gradually phased-in implementation approach. Begin with high impact endpoints (e.g., domain controllers, application servers, databases), followed by any remaining support systems, and ending with any remaining user workstations or endpoints.

- **Maintain proper encryption key management.** Key management is vital to the security of LMR systems that use encryption. Key management is creating, distributing, using, archiving, and destroying encryption keys in an LMR system. Encryption allows the authorized users to securely send and receive voice, data, and video communications without the risk of interception. Proper key management also fosters secure interoperability between different agencies. In addition, regularly updating encryption keys ensures the integrity of the encryption system and prevents using outdated or compromised keys on the LMR system.
- **Develop an external reporting structure (e.g., outside partners, vendors, government and industry responders, technical advisors, and law enforcement).** Identify the external stakeholders who could assist with the response or should be notified. Document the order in which they should be contacted, per the organization's policies and procedures and federal and state regulations. Build these relationships in advance and understand what is required to obtain support.[8]

## *Detect*

Knowing when an attack occurs could further minimize damage to the LMR system instead of discovering an intrusion much later in the attack stage. Additionally, once the threat is detected, having an established plan in place will potentially reduce the impact on the system.

- **Continually scan for anomalies and events.** The difference between normal and abnormal activity may only get detected if the proper scanning mechanisms are in place. Consider establishing a network baseline to detect anomalies.
- **Develop detection processes.** Establish well-defined roles and responsibilities for detection procedures; test the procedures to ensure awareness of anomalous activities.

## *Respond*

Establishing the proper response to cyberattacks may reduce the impact and restore the LMR system securely and promptly.

- **Implement the predetermined incident response plan and follow the established internal and external reporting structure.** Implement the established guidelines and follow the steps outlined in the plan. Be prepared to potentially deviate or adjust the procedures as the cyber incident could render parts of the plan inapplicable. Follow the agreed-upon reporting procedures and communications channels to ensure all updates are captured and understood.

[8] For example, CISA (https://us-cert.cisa.gov/report) and the Federal Bureau of Investigation (https://www.ic3.gov/Home/IndustryAlerts) provide dedicated hubs for helping respond to cyber and critical infrastructure attacks. Both have resources and guidelines on when, how, and to whom an incident should be reported to receive assistance. Organizations should also file a formal report with local law enforcement to obtain an official record of the incident in addition to reporting internally.

- **Leverage system impact assessments to prioritize resources and identify which systems must be recovered first.** The analysis helps to identify and prioritize critical systems, information, and assets. This information determines contingency requirements and priorities for essential information and services. It also allows planning for disruption impacts and identifies allowable outage times.
- **Coordinate with internal and external partners.** Cyberattacks could impact more than just one organization. As a part of the response step, it is imperative to keep intra-and extra-organizational partners informed and coordinate as needed on specific response actions. Be prepared to brief partners on status of the cyber incident, existing roles and responsibilities, as well as any support expected from them.
- **Leverage containment measures to limit the impact of cyber incidents when they occur.** Communicate and execute the predetermined cyber incident response plan, such as isolating a network segment of infected workstations or switching to different communication methods to reroute traffic to unaffected infrastructure. Test LMR systems to ensure they are operational and configured securely after the incident is resolved. Communicate the damage done and the improvements applied to recovery planning and action to build trust and a culture of growth and resilience within the organization.[9]

## *Recover*

Recovery is important to getting the LMR system back online and preventing future cybersecurity incidents. Below are several recommendations for a speedy recovery.

- **Execute the recovery plan.** Develop and implement appropriate activities to maintain resilience plans and restore any capabilities or services impaired due to a cybersecurity event.
- **Leverage after-action reports to improve continuity planning.** After-action reports often provide valuable insights that could strengthen future cyber responses. Conduct after-action reviews and communicate findings throughout the organization. Actively solicit feedback from internal and external stakeholders. Incorporate feedback into future continuity planning, standard operating procedures, and training and exercises.
- **Maintain process improvements.** Incorporate lessons learned into future activities to improve the recovery planning processes and strategies. Train response personnel on the latest security, resiliency, continuity, and operational practices and maintain in-service training as new technology and methods are available.
- **Coordinate communications restoration.** Coordinate restoration activities with internal and external parties, such as coordinating centers, internet service providers, owners of attacking systems, victims, response partners, and vendors.

[9] Review available technical guidance, such as *Technical Approaches to Uncovering and Remediating Malicious Activity* from CISA (AA20-245A https://us-cert.cisa.gov/ncas/alerts/aa20-245a), a collaborative advisory of five nations (Australia, Canada, New Zealand, the United Kingdom, and the United States) that highlights technical details to find malicious activities and related mitigation steps and best practices.

## Next Steps

LMR system owners are encouraged to assess their systems and determine their vulnerabilities to cyberattacks comprehensively. Recognizing the importance of cybersecurity and the impacts on LMR systems will help mitigate potential cyber risks and improve LMR system resiliency. Review the NIST Cybersecurity Framework and follow the below six best practices to help secure LMR systems.

1. **Acknowledge that LMR systems are susceptible to vulnerabilities and attacks just like other IT infrastructure.** As such, assess the LMR system network components/security posture and recognize the various forms of cyber threats to the network.
2. **Develop and implement cyber incident and vulnerability response plans** that establish the policies and procedures to provide identification, evaluation, remediation, reporting, and notification of incidents and vulnerabilities affecting systems, data, and networks.
3. **Implement regular security patching and updates on all operating systems and software** to ensure physical and virtual assets are secure. Remove any unauthorized or outdated component from the system that could provide insecure access to the LMR network. Maintain proper encryption protocols and key management policies.
4. **Regularly scan the network for abnormal activities and develop security violation detection processes** that the system users and administrators know.
5. **Respond to cyberattacks immediately** to reduce impacts on the system. Threats can be mitigated by having a well-developed incident response and disaster recovery plan that prioritizes resources.
6. Get the LMR system back online as soon as possible with a **comprehensive recovery plan** that is periodically tested to ensure system users and technicians are prepared to respond to cyberattacks before they occur.

## Appendix A: Example LMR Cybersecurity Resources

- The Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Essentials Toolkit (cisa.gov/publication/cyber-essentials-toolkits)
- Public Safety Communications: Ten Keys to Improving Emergency Alerts, Warnings & Notifications (cisa.gov/publication/alerts-and-warnings)
- CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (us-cert.cisa.gov/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability)
- CISA's Interoperable Communications Technical Assistance Program (cisa.gov/safecom/ictapscip-resources)
- Encryption Documents (cisa.gov/safecom/encryption)
  - Guidelines for Encryption in Land Mobile Radio Systems
  - Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems
  - Developing Methods to Improve Encrypted Interoperability in Public Safety Communication
  - Considerations for Encryption in Public Safety Radio Systems
  - Determining the Need for Encryption in Public Safety Radios Fact Sheet
  - Encryption Key Management Fact Sheet
  - Operational Best Practices for Encryption Key Management
- Land Mobile Radio and Broadband Evolution Webpage (cisa.gov/publication/lmr-and-broadband-evolution)
  - Public Safety Communications Evolution Brochure
  - Interoperability Planning for Wireless Broadband
  - Modeling and Analysis for Public Safety Broadband
- CISA Communications and Cyber Resiliency Toolkit (cisa.gov/publication/communications-resiliency)
  - Radio Frequency Interference Best Practices Guidebook
  - Public Safety Communications Network Resiliency Self-Assessment Guidebook
  - Cyber Risks to Public Safety: Ransomware
  - Public Safety Communications Dependencies on Non-Agency Infrastructure and Services
- SAFECOM Funding Resources Webpage (cisa.gov/safecom/funding)
  - Funding and Sustaining Land Mobile Radio (LMR) Trio, Part 1: Educating Decision-Makers on LMR Fundamentals
  - Funding and Sustaining LMR Trio, Part 2: Educating Decision-Makers on LMR Technology Issues
  - Funding and Sustaining LMR Trio, Part 3: Educating Project and Acquisition Managers on Project 25
  - Funding and Sustaining LMR Systems Brochure
  - Promoting the Importance of Funding and Sustaining LMR Action Memorandum
- Motorola Solutions: *LMR Cybersecurity – Bridging the Disconnect Between Perception and Action* (motorolasolutions.com/content/dam/msi/docs/en-xu/public-safety/lmr_systems_cybersecurity_trends.pdf)
- Motorola Solutions: *The Global State of LMR System Management* (hankeysradioinc.com/downloads/motorola/motorola-solutions-lmr-services-survey-report.pdf)
- Idaho National Laboratory: *Cyber Security Concerns for Sharing Distributed Antenna Systems* (inldigitallibrary.inl.gov/sites/sti/sti/Sort_3432.pdf)
- Information and Communications Technology Supply Chain Risk Management (cisa.gov/supply-chain)

## Appendix B: Cyber Risks to LMR Mitigation Overview

| Step One: Identify |
| --- |
| • *Identify what is on the network* |
| **Step Two: Protect** |
| • *Develop incident response and disaster recovery plans outlining roles and responsibilities*<br>• *Develop an internal reporting structure to detect, communicate, and contain attacks*<br>• *Keep all software, including operating systems, applications, and firmware, up to date*<br>• *Implement secure configurations for all hardware and software assets so that both physical and virtual assets are protected*<br>• *Remove unsupported or unauthorized hardware and software*<br>• *Create application integrity, allowlist, and blocklist policies so that only approved software can operate on the system*<br>• *Maintain proper encryption key management*<br>• *Develop an external reporting structure (e.g., outside partners, vendors, government and industry responders, technical advisors, law enforcement)* |
| **Step Three: Detect** |
| • *Continually scan for anomalies and events*<br>• *Develop detection processes* |
| **Step Four: Respond** |
| • *Implement the predetermined incident response plan and follow the established internal reporting structure*<br>• *Leverage system impact assessments to prioritize resources and identify which systems must be recovered first*<br>• *Coordinate with internal and external partners*<br>• *Leverage containment measures to limit the impact of cyber incidents when they occur* |
| **Step Five: Recover** |
| • *Execute the recovery plan*<br>• *Leverage after-action reports to improve continuity planning*<br>• *Maintain process improvements*<br>• *Coordinate communications restoration* |