






# ASTRO 25 SYSTEMS AND THE NIST CYBERSECURITY FRAMEWORK

## INDUSTRY LEADING SUPPORT EVERY STEP OF THE WAY

Too often, cybersecurity decisions are made with a “check the box” mindset driven by the need to meet compliance requirements. With the surging frequency and sophistication of today’s cyber threats, this is no longer sufficient.

Today, organizations must adopt a holistic and organization-wide risk-based approach to security, with the National Institute of Standards and Technology (NIST) Cybersecurity Framework at its core. This approach focuses on mitigation options, continuous monitoring, diagnosis and remediation to evolve security practices. While federal agencies responsible for the safety of the nation’s critical technical infrastructure are required to follow the framework, all agencies and organizations can rely on it for a more robust and effective approach to cybersecurity. The [Motorola Solutions Trust Center](#) provides information about how we deliver security and privacy via our products and services.

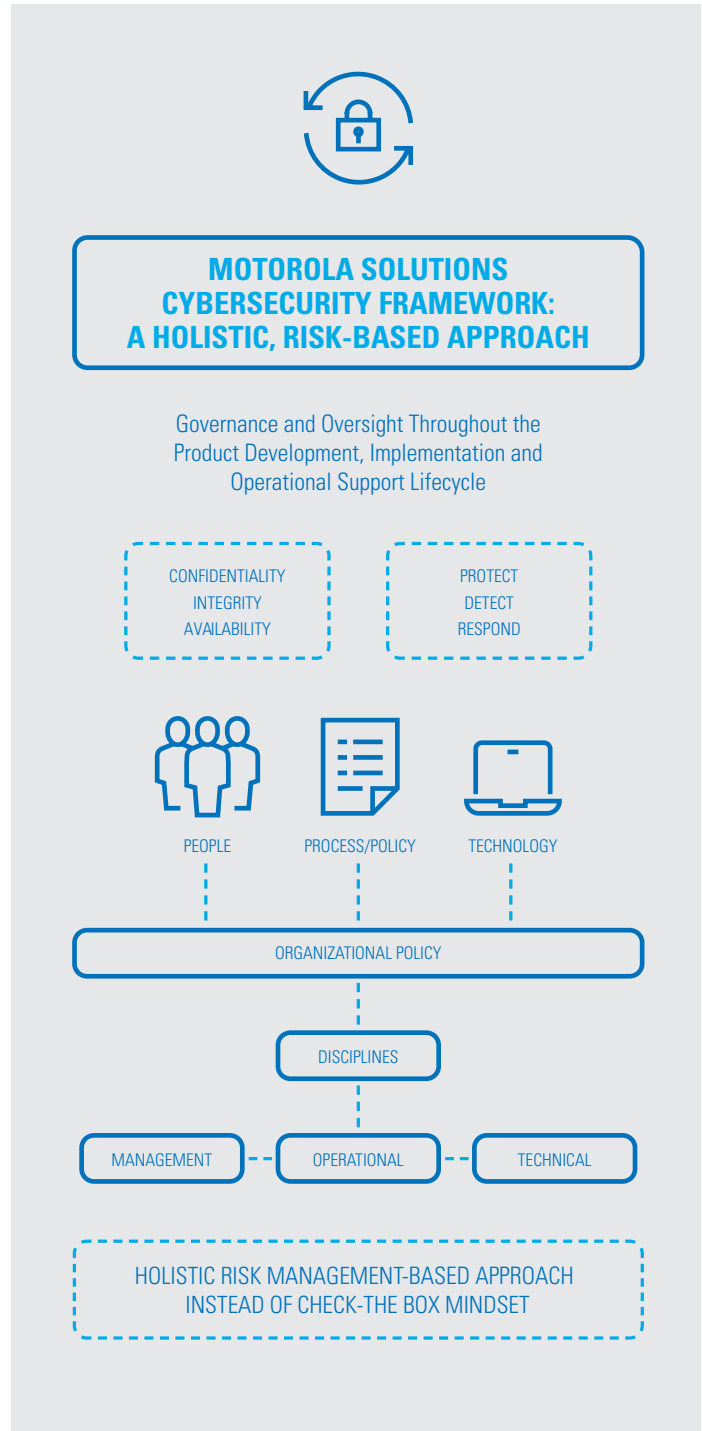
CYBERSECURITY FRAMEWORK	SYSTEMATIC ANALYSIS AND PLAN
 <b>IDENTIFY</b> Access Risks	<ul style="list-style-type: none"><li>• Provide a thorough risk analysis</li><li>• Uncover potential vulnerabilities</li></ul>
 <b>PROTECT</b> Develop Safeguards	<ul style="list-style-type: none"><li>• Develop policies and procedures</li><li>• Implement appropriate access and auditing controls</li></ul>
 <b>DETECT</b> Make Timely Discoveries	<ul style="list-style-type: none"><li>• Continuous monitoring 24x7x365</li><li>• Enable auditing capabilities</li></ul>
 <b>RESPOND</b> Take Action	<ul style="list-style-type: none"><li>• Establish a robust response plan</li><li>• Create, analyze, triage and respond to detected events</li></ul>
 <b>RECOVER</b> Restore Functionality	<ul style="list-style-type: none"><li>• Institute a recovery plan</li><li>• Create improvements to prevent future attacks</li></ul>

# A TRUSTED, VALUE-ADD PARTNER

Motorola Solutions uses a risk-based approach throughout our entire product development, implementation and operational support lifecycle. We strongly believe in three foundational pillars of cybersecurity: confidentiality, integrity and availability. We address these pillars with the application of protection, detection and response controls built with industry-leading people, processes and technology.

For ASTRO 25 systems, our holistic approach to cybersecurity includes a range of services that help personalize your experience and meet your exact needs, including:

- **Motorola Solutions Federal Government Cybersecurity Team Support.** CISSP-certified professionals help enhance system security during implementation and throughout the system lifecycle.
- **System Staging Custom Configuration.** Our cybersecurity technicians work with you to customize security configurations based on engineering- approved alterations. This approach minimizes risks to the operation, performance and warranty support status of the system.
- **System Vulnerability Scanning Options.** Our cybersecurity technicians perform System Staging, System Field and Recurring System Vulnerability Scanning. For Federal agencies, these scans are followed up by a feedback report that addresses Nessus “Critical” and “High” findings.
- **Security Monitoring Service.** Experienced, specialized security technologists with years of experience working with communications networks like yours provide uninterrupted monitoring of the radio network security elements to detect, analyze and respond remotely or on-site to security events.
- **Security Update Service (SUS) and Security Update Remote Delivery Service.** We provide peace of mind that the 3rd party software security patches are vetted for issues before they are applied to your live ASTRO 25 system. These 3rd party patches include weekly anti-malware definition updates, monthly Microsoft Windows updates and other operating system patches as they are released.
- **Cybersecurity Assessment Service.** Motorola Solutions’ cybersecurity professional services provide a comprehensive and systematic process for identifying, assessing and managing cybersecurity risk throughout enterprise systems. We provide a comprehensive assessment of your attack surface profile; a cost/benefit evaluation and detailed remediation recommendations.
- **ASTRO 25 Application Solutions Center.** Located in Schaumburg, IL, the solutions center enables application suppliers to validate their application end-to-end in an ASTRO 25 system lab environment. The result? You are assured a higher quality product.



# ASTRO 25: COMPREHENSIVE SUPPORT FOR EVERY PHASE OF THE NIST CYBERSECURITY FRAMEWORK

Motorola Solutions ASTRO 25 systems help you follow every phase of the NIST framework. We use a risk-based approach throughout our entire ASTRO 25 product development, implementation and operational support lifecycle. With Motorola Solutions as your trusted cybersecurity partner, you free up more time and resources to focus on your core mission.



## IDENTIFY Access Risks

### Asset Management

- Asset & Role Management
- Open Source Review Board
- System Configuration Artifacts

### Business Environment

- Market Verticals: Supporting all verticals from Federal, Nationwide, State and Local Public Safety systems to small single site systems
- Customer Engagements: Strong customer engagement to identify requirements
- Release & Product Lifecycle Strategies: Support roadmaps for releases with supporting product announcements, Motorola Solutions Cybersecurity Risk Management Framework for vendors

### Governance

- Product & Services Governance
- Business Risk Owner

### Cybersecurity Risk Assessment

- System & Product Risk Assessments: Against Motorola Solutions' Minimum Viable Secure Product (MVSP) requirements, NIST CSF
- Secure Design Review and Audit
- Vulnerability Scanning & Remediation
- Threat Intelligence & Communication
- Customer Self-Assessments: Response reports to customers' pen test reports
- In-Field Security Assessments: On-site system assessments

### Risk Management Strategy

- Cybersecurity Risk Management
- Business Risk Owner
- Risk Registry

### Supply Chain Risk Management

- Supplier Qualification and Assessment
- Supply Chain Controls



## **PROTECT** Develop Safeguards

### **Identity Management, Authentication & Access Control**

- Subscriber Authentication: APCO P25 standard-based
- Agency Partitioning, Role-Based Access Control: Supporting multi-agency systems and separation of duties
- Centralized identity access management using Active Directory (AD) for ASTRO 25 Systems
- FIPS 201 based (smart card) Multi-Factor Authentication: For Linux, Windows, Embedded OS platforms and SSO Web Applications
- Multi-Factor Authentication solution for Service Access
- RADIUS Authentication for embedded operating systems
- SNMPv3-based Authentication from all devices

### **Platform and Application Security**

- OS platforms configuration hardening per DISA STIG based on NIST SP 800-53 Controls
- Application configurations hardening per DISA Application Security and Development STIG based on NIST SP 800-53 Controls

### **McAfee Endpoint Security Threat Protection Service**

Centrally managed service that provides:

- Real time Exploit prevention against zero-day threats and Network based file-less and scripted attacks
- Browser Protection against web malicious and unauthorized sites based threats
- Dynamic Application Containment against ransomware and grayware attacks
- Roll back remediation against malware and ransomware
- Intelligent Adaptive Virus scanning
- Host intrusion firewall Blocks Hostile Network (inbound/outbound) attacks
- Super Agent Distributed Repositories (SADR)

### **Awareness & Training**

- Security Training for Motorola Solutions Personnel
- Roles & Responsibilities
- Training Available for Customers

### **Data Security**

- Air Interface Encryption: APCO P25 standard-based
- End-to-End Encryption for Voice & Data: APCO P25 standard-based, all console products for voice and for the short data text service and packet data
- Ethernet Site Link Encryption: Standard IPsec AES/SHA-2 encryption
- Encryption of Sensitive Data: Encryption of key material per APCO P25 / FIPS 140-2 recommendations
- FIPS 140-2 Level 3 Hardware Security Module (HSM) protected key storage for PKI high-speed signature and hardware key generation operations

### **Info Protections & Procedures**

- Secure Development Lifecycle
- Vulnerability Management: Vulnerability investigation & impact analysis and risk-based decision process
- Change Control Management
- Backup & Restore: Automated for all ESU (Enhanced Software Upgrade) capable products
- Off-site NAS storage support for Alternate Storage Site Contingency

### **Maintenance**

- Pre-tested Patch & Anti-malware Updates
- Regular Maintenance Release
- Product Specific Releases with Emergency Releases when needed

### **Security Update Service**

- Common Hardening Benchmarks: DISA STIG-based
- Anti-malware Protection: For all Linux and Windows-based devices
- Network Enforcements: Covering security boundaries between RNI (Radio Network Infrastructure), DMZ, CEN (Customer Enterprise Network) and to the Internet





## **DETECT** Make Timely Discoveries

### **Detect Anomalies & Events**

- Centralized Anti-Malware Reporting: System wide, centralized
- Centralized Log Collection: Logs from system elements
- Field Security Assessments
- Real-time Intrusion Detection System

### **Security Continuous Monitoring**

- Event Forwarding: All syslog events can be forwarded to two customer-defined destinations
- Northbound Alarm Forwarding: SNMPv3-based, supports authentication and encryption

### **Detection Process**

- Abuse/Misuse Case Testing
- In-Field Security Assessment Services

### **Auditing & Logging Capabilities**

- Auditing: From all Linux and Windows-based devices
- Auditing: From applications
- syslog: From all Linux and Windows-based devices
- syslog: From all network transport and RF Site devices
- syslog: From all security-dedicated products A/V, Authentication Manager



## **RESPOND** Take Action

### **Response Planning**

- Defined notification processes in the event of security incident detection
- Defined roles & responsibilities

### **Analysis**

- Vulnerability Investigation
- Threat Intelligence Analysis

### **Mitigation**

- Global Customer Issue Resolution Policy
- Global Incident Management Procedure
- Technical Notifications & Updates

### **Improvements**

- Secure Development Lifecycle
- Feeding findings and remediations back into the development cycle



## RECOVER

Restore  
Functionality

### Recovery Planning

- Defined Recovery Procedures: Part of the system design and documentation supported by install methods and backup & restore features
- Motorola Solutions On-Site Support
- Redundancy: System design with both geo and local redundancy
- Backup & Restore: Baseline support or full support options

### Improvements

- Lessons Learned: Feeding findings and remediations back into the development cycle
- Process Improvements: Feeding findings and remediations back into the development cycle

### Communications

- Cybersecurity Notices
- Motorola Technical Notifications (MTN)

Learn more about ASTRO 25 radio systems  
at [www.motorolasolutions.com/astro](http://www.motorolasolutions.com/astro)



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. [motorolasolutions.com](http://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. © 2020 Motorola Solutions, Inc. All rights reserved. 10-2020