







# MOTOROLA SOLUTIONS MOTOTRBO 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 government agencies responsible for the safety of their 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.

Note: Our MOTOTRBO portfolio is a global offering. Features may vary depending on the region and support agreements. The following is a high level description of the NIST Cybersecurity Framework that MSI applies to MOTOTRBO portfolio product development.

CYBERSECURITY FRAMEWORK	SYSTEMATIC ANALYSIS AND PLAN
 <b>IDENTIFY</b> Assess Risks	<ul style="list-style-type: none"><li>• Perform a thorough risk analysis</li></ul>
 <b>PROTECT</b> Develop Safeguards	<ul style="list-style-type: none"><li>• Develop policies and procedures</li><li>• Implement appropriate access controls</li></ul>
 <b>RESPOND</b> Take Action	<ul style="list-style-type: none"><li>• Enable establishment of a robust response plan</li></ul>
 <b>RECOVER</b> Restore Functionality	<ul style="list-style-type: none"><li>• Enable establishment of a recovery plan</li><li>• Product &amp; solution improvements to prevent future attacks</li></ul>

# A TRUSTED 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 and response controls built with industry-leading people, processes and technology.

MOTOTRBO systems maintain security practices based on enterprise needs.

- **System Vulnerability Scanning.**

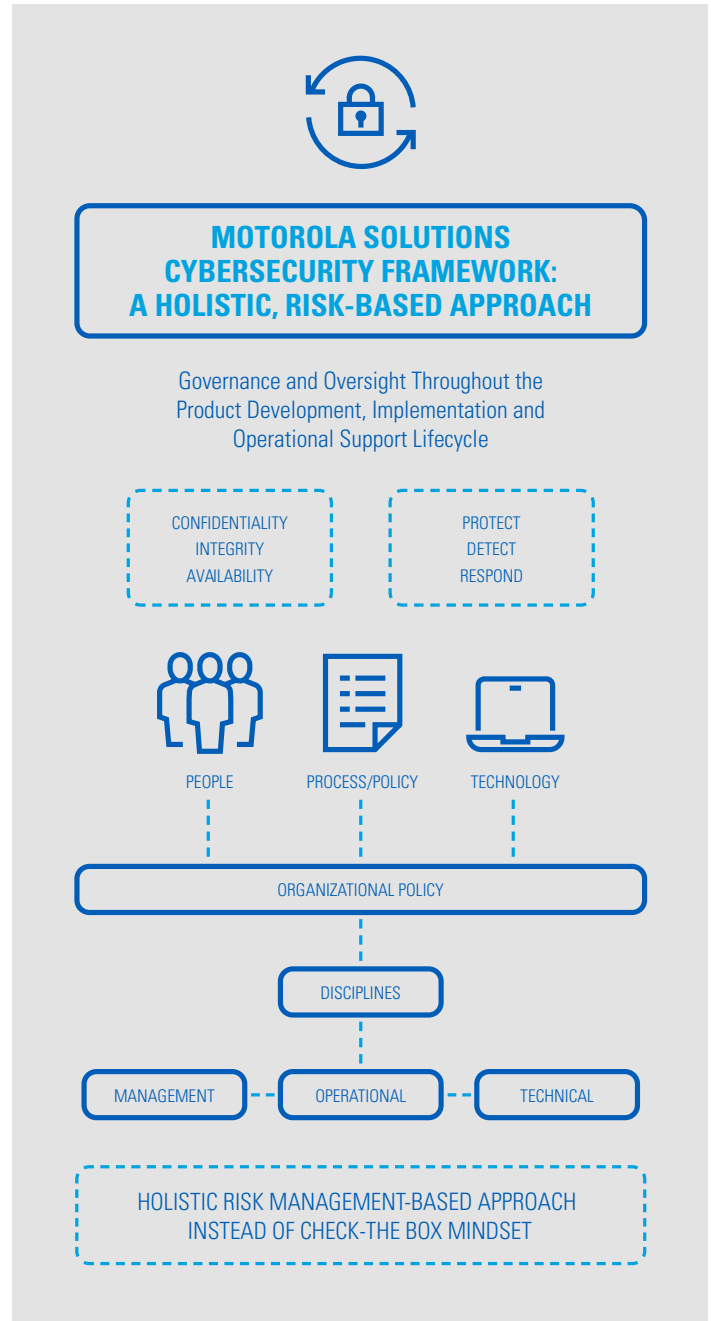
Our cybersecurity development engineers perform System Vulnerability Scanning using industry standard tools like Nessus. MSI performs the vulnerability scanning before the system release launch. These scans are followed up by a remediation plan based upon a holistic risk-based approach.

- **Security Update.**

Third-party software security updates are vetted for issues before they are applied to your MOTOTRBO system. These third-party updates include operating system updates. Security updates are included in MOTOTRBO system software releases.

- **Cybersecurity Foundation Built in Partnership.**

We engage with authorized application providers on cybersecurity best practices, standards and knowledge sharing. Motorola Solutions establishes a cybersecurity foundation through the procurement process for applications provided by the sold and supported program.





## MOTOTRBO: COMPREHENSIVE SUPPORT FOR THE NIST CYBERSECURITY FRAMEWORK

Motorola Solutions MOTOTRBO systems strictly adhere to the NIST framework. We use a risk-based approach throughout our entire MOTOTRBO product development, implementation and operational support lifecycle. As your trusted cybersecurity partner, we can help you free up more time and resources to focus on your core mission.



### **IDENTIFY** Assess Risks

#### **Asset Management**

- Open Source Review Board
- System Configuration Artifacts

#### **Business Environment**

- Market Verticals: Supporting all verticals from Commercial, 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 performed against Motorola Solutions' secure product requirements which are based upon the NIST Cybersecurity Framework
- Secure Design Review
- Vulnerability Scanning & Remediation
- Threat Intelligence & Communication

#### **Risk Management Strategy**

- Cybersecurity Risk Management
- Business Risk Owner
- Risk Registry

#### **Supply Chain Risk Management**

- Supplier Qualification
- Supply Chain Controls



## **PROTECT** Develop Safeguards

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

- Authentication: DMR standard-based
- Restricted Access to System (RAS) feature

### **Awareness & Training**

- Security Training for Motorola Solutions Personnel
- Training Available for Customers

### **Data Security**

- Packet Encryption: DMR standard-based
- End-to-End Encryption for Voice: DMR standard-based.
- Ethernet Site Link Encryption: All links can be encrypted per standard IP VPN technology for ex., IPSec, SHA-2 encryption

### **Info Protections & Procedures**

- Secure Development Lifecycle
- Vulnerability Management: Vulnerability investigation & impact analysis and risk-based decision process
- Change Control Management
- Common Hardening Benchmarks: DISA STIG-based

### **Maintenance**

- Product Specific Releases with Emergency Releases when needed



## **RESPOND** Take Action

### **Communications**

- Roles & Responsibilities
- Coordinated Communications

### **Analysis**

- Vulnerability Investigation
- Threat Intelligence Analysis

### **Mitigation**

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

### **Improvements**

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



## **RECOVER** Restore Functionality

### **Recovery Planning**

- Recovery Procedures: Part of the system design and Documentation supported by install methods
- On-site support
- Geographical & Local Redundancy: System design with both geo and local redundancy
- Backup & restore support

### **Improvements**

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

### **Communications**

- Customer engagement with MSI and partners



**MOTOROLA SOLUTIONS**