








# MOTOROLA SOLUTIONS 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.

CYBERSECURITY FRAMEWORK	SYSTEMATIC ANALYSIS AND PLAN
 <b>IDENTIFY</b> Assess Risks	<ul style="list-style-type: none"><li>• Inventory critical assets and systems</li><li>• Provide 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 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>



## WHAT IS A RISK-BASED STRATEGY?

A Risk-based strategy begins with the process of identifying and reviewing the complete range of risks an organization faces. By first assessing risks, you become actively aware of where uncertainty surrounding events or outcomes exists. Then, based on risk prioritization, steps are identified to reduce risk or remediate a situation to protect the organization, people and assets concerned. Forward-looking security conscious organizations are shifting to this risk mindset, focusing on mitigation options, continuous monitoring, diagnosis and remediation to evolve security practices.

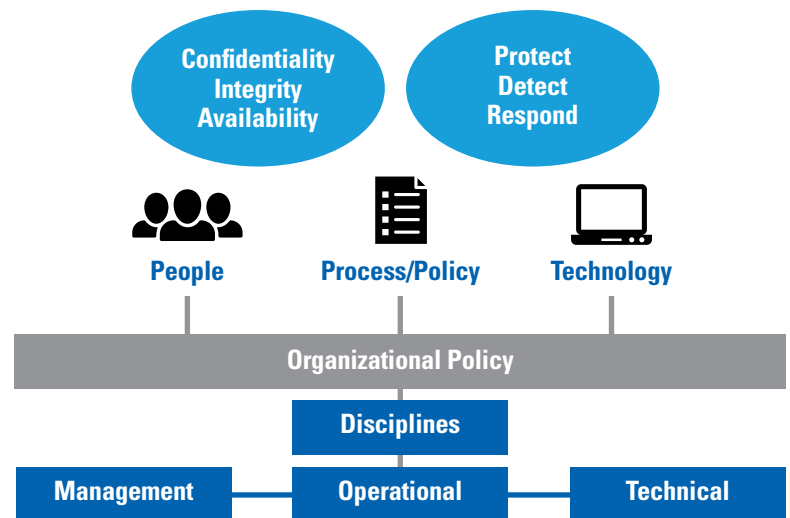
## A TRUSTED, VALUE-ADD PARTNER

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 cyber security: 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.

That is why we created a Motorola Solutions Products & Services Cybersecurity Team to oversee and guide cybersecurity across all of our products, solutions, and services. The team holds top industry cybersecurity certifications and stays sharp with comprehensive, ongoing training. It provides input on the entire range of Motorola Solutions cybersecurity products and services, from security monitoring solutions and notification services to security assessments, patching, and updating services.

### Motorola Solutions Cybersecurity Framework: A Holistic, Risk-Based Approach

Governance and Oversight Throughout the Product Development, Implementation and Operational Support Lifecycle








Holistic Risk Management-based approach instead of Check-in-the-Box mindset

# COMPREHENSIVE SUPPORT FOR EVERY PHASE OF THE NIST CYBERSECURITY FRAMEWORK

Motorola Solutions offers an end-to-end cybersecurity solution, with products and services encompassing every phase of the NIST framework. With Motorola Solutions as your trusted cybersecurity partner, you free more time and resources to focus on your core mission.

## PRODUCTS AND SERVICES

 <p><b>IDENTIFY</b></p>	<p><b>Asset Management</b></p> <ul style="list-style-type: none"> <li>• Systems staging centers inventory database</li> <li>• Open Source Review Board provides approval for use of open source documents</li> </ul> <p><b>Business Environment</b></p> <ul style="list-style-type: none"> <li>• Strategy planning and priorities aligned to supported vertical markets</li> </ul> <p><b>Governance</b></p> <ul style="list-style-type: none"> <li>• Oversight board handling Governance, Risks and Compliance by creation of policies, standards and procedures</li> </ul>	<p><b>Cybersecurity Risk Assessment (Onsite)</b></p> <ul style="list-style-type: none"> <li>• Secure Design Review and Audit</li> <li>• Vulnerability scanning, remediation, and intelligence</li> </ul> <p><b>Risk Management Strategy</b></p> <ul style="list-style-type: none"> <li>• Dedicated team actively monitoring and collecting threat information</li> </ul> <p><b>Supply Chain Risk Management</b></p> <ul style="list-style-type: none"> <li>• Supplier Qualification and Assessment</li> </ul>
 <p><b>PROTECT</b></p>	<p><b>Identity Management, Authentication &amp; Access Control Awareness &amp; Training</b></p> <ul style="list-style-type: none"> <li>• Extensive Security Training</li> </ul> <p><b>Data Security</b></p> <ul style="list-style-type: none"> <li>• Appropriate controls based on policies and risk strategy</li> </ul>	<p><b>Info Protections &amp; Procedures</b></p> <ul style="list-style-type: none"> <li>• Secure Software Development Lifecycle</li> </ul> <p><b>Security Update Service</b></p> <ul style="list-style-type: none"> <li>• Pre-tested Patch and Anti-Virus Updates</li> </ul> <p><b>Protective Technologies</b></p> <ul style="list-style-type: none"> <li>• Common Hardening Benchmarks</li> </ul>
 <p><b>DETECT</b></p>	<p><b>Detect Anomalies &amp; Events</b></p> <ul style="list-style-type: none"> <li>• Abuse/Misuse case testing</li> <li>• Audit Logging</li> <li>• Security Assessment Services</li> </ul>	<p><b>Security Continuous Monitoring</b></p> <ul style="list-style-type: none"> <li>• Threat intelligence to detect and alert on cyber threats</li> <li>• Vulnerability assessments to identify, quantify and prioritize vulnerabilities</li> </ul>
 <p><b>RESPOND</b></p>	<p><b>Response Planning</b></p> <ul style="list-style-type: none"> <li>• Defined notification processes and procedures in the event of security incident detection</li> </ul> <p><b>Communications</b></p> <ul style="list-style-type: none"> <li>• Motorola Technical Notifications (MTN)</li> </ul> <p><b>Analysis</b></p> <ul style="list-style-type: none"> <li>• Vulnerability Investigation</li> </ul>	<p><b>Mitigation</b></p> <ul style="list-style-type: none"> <li>• Security Operations Centers and Call Centers can remotely access the supported systems in order to quickly take action</li> </ul> <p><b>Improvements</b></p> <ul style="list-style-type: none"> <li>• Via patches or compensating controls</li> </ul>
 <p><b>RECOVER</b></p>	<p><b>Recovery Planning</b></p> <ul style="list-style-type: none"> <li>• Assisted System Restoration</li> <li>• Loaner Program</li> </ul> <p><b>Improvements</b></p> <ul style="list-style-type: none"> <li>• Lessons Learned</li> <li>• Enhance solution verification and validation</li> </ul>	<p><b>Communications</b></p> <ul style="list-style-type: none"> <li>• Cybersecurity Notices</li> <li>• Motorola Technical Notifications (MTN)</li> </ul>



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. © 2019 Motorola Solutions, Inc. All rights reserved. 05-2019