Solution Brief

ASTRO Federal Cybersecurity Services

Ensure compliance and achieve authority to operate

Cybercrime continues to grow and federal information systems are a prime target. In response, U.S. Federal Government organizations now have many detailed and specific requirements for cybersecurity compliance which are mandated by legislation such as the Federal Information Security Modernization Act (FISMA) of 2014. As a key element of the FISMA Implementation Project, the National Institute of Standards and Technology (NIST) developed an integrated Risk Management Framework (RMF) which effectively brings together all of the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.

The NIST Risk Management Framework (RMF) consists of 7 steps, which are:

PREPARE	Essential activities to **prepare** the organization to manage security and privacy risks
CATEGORIZE	**Categorize** the system and information processed, and transmitted based on an impact analysis
SELECT	**Select** the set of NIST SP 800-53 controls to protect the system on risk assessment(s)
IMPLEMENT	**Implement** the controls and document how controls are deployed
ASSESS	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
AUTHORIZE	Senior official makes a risk-based decision to **authorize** the system (to operate)
MONITOR	Continuously **monitor** control implementation and risks to the system

The Risk Management Framework approach to cybersecurity accreditation is collaborative between Motorola Solutions and Federal agencies. With over 15 years of experience in Federal Cyber Services, Motorola Solutions is extremely well-equipped to help you navigate the process toward achieving accreditation and Authority To Operate (ATO) your ASTRO® radio system. Our cyber experts are specifically trained to provide you with the documentation, implementation, assessments and recommendations related to the security of your ASTRO radio system.

MOTOROLA SOLUTIONS

RMF Documentation and Hardening

Establish a baseline for cybersecurity protection

Documentation is among the initial stages of our ASTRO RMF accreditation services. This documentation is used to establish a baseline of vendor-provided documentation to eliminate ambiguity and helps to drive subsequent steps.

- Document a high level view of the ASTRO system
- Define the Accreditation Boundary and items contained within
- Document the ports and protocols that communicate within the Accreditation Boundary

ASTRO System Hardening ensures the devices are configured to the current available configurations, typically defined by the latest DISA Security Technical Implementation Guides (STIG). Hardening applies configuration settings that help enforce STIG compliance and applies organization specific login banners on devices.

Vulnerability Scanning

Identify vulnerabilities and weaknesses

The primary objective of the Vulnerability Scan is to identify missing patches and other weaknesses. Patching is a critical factor in maintaining a secure system and reducing the vulnerabilities that could be exploited. Vulnerability scanning is performed as part of preparing an accreditation package as well as ongoing regular scanning to support RMF Continuous Monitoring of the system security posture. Vulnerability scanning includes:

- A Nessus vulnerability scan of all IP connected devices within the Accreditation Boundary
- A set of files and reports resulting from the scans
- Cybersecurity findings analysis
- Remediation reporting for “Critical, High, Medium” severity findings

NIST SP 800-53 Controls Compliance

Verify policies and procedures

Controls Compliance is used to determine the Confidentiality, Integrity and Availability (CIA) Categorization of various controls used on the ASTRO radio system. The assessment is performed per NIST SP 800-53 guidelines on a baseline ASTRO radio system, while also responding to controls that may be dependent on the system’s technical capabilities.

The majority of the controls are considered administrative and operational which require policies and procedures with evidence that they are being followed. Our Controls Compliance services provide assistance for responding to these controls. Creation of customer-specific policy and procedure documentation, or other artifacts to address non-technical controls, is not included in this service.

The results of controls compliance evaluation are compiled into a standard template that lists:

- Control responsibility owner
- System compliance status
- Control implementation information

STIG SCAP Scanning

Automatically scan for DISA STIG compliance

Defense Information Systems Agency (DISA) Security Technical Implementation Guidelines (STIGs) and Security Requirement Guides (SRGs) outline criteria for hardening configurations of servers, workstations and applications to reduce vulnerabilities. This hardening involves configuration settings that are intended to improve security. DISA typically releases updates to STIGs and SRGs on a quarterly basis. Periodic scanning provides compliance against applicable DISA Benchmarks to satisfy frequent monitoring. We offer Nessus based Automatic Security Content Application (SCAP) scans on applicable ASTRO system devices at a cadence defined by you. The output is a spreadsheet report format that includes:

- Cybersecurity Findings analysis
- Mitigation Statements
- Remediation reporting for CAT I, II and III findings

STIG Audit

Manually verify all applicable DISA STIGS

STIG Audit consists of the validation of STIGs applicable to ASTRO system devices using DISA STIGs benchmarks, and tools. STIG audits include a combination of automated and manual checks with manual checks targeted at devices for which there are no automated tools. The STIG audit service meets annual configuration audit requirements which may be required in the RMF Monitoring Step.

- Checklists from audits
- Plan of Actions and Mitigations (POA&M)
- Raw file type artifacts produced by STIG Validation tools

Smart Card MFA Implementation Support

Ease smart card implementation

On the surface, using a smart card to authenticate seems like a simple thing. You put your card in the reader attached to the computer being accessed, enter the correct PIN or passphrase, and you are logged in. Behind the scenes, however, is a much more complicated process. The policies for the administration and use of smart cards for authentication vary widely.

Each implementation of Common Access Card/Personal Identity Verifications (CAC/PIV) varies by individual needs of the organization. Our Smart Card MFA implementation support helps to ensure a successful implementation of CAC\PIV on your ASTRO radio system with the following services:

- Smart Card MFA implementation
- Training on CAC/PIV functions
- Testing of smart cards/tokens
- Installation-related MFA support

Cybersecurity Consulting

Gain access to ASTRO cybersecurity experts

Cybersecurity can be complex, but we have experts who can help. Our advisory services give you access to distinguished and technical expertise personnel who meet 8570 certification requirements and possess necessary security clearances. They have extensive knowledge of ASTRO compliance to Federal Government cybersecurity requirements including, but not limited to, DHS 4300A and NIST SP 800-53.

To learn more, visit: **www.motorolasolutions.com/astro-security**

MOTOROLA SOLUTIONS

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

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. 03-2024 [CK08]