WHITE PAPER

MOTOROLA

Information Assurance For ASTRO®25 Networks

Securing Your Mission Critical Communications

The security of voice and data communications is a top priority in any organization. This is especially true for government agencies that rely upon these systems for the safety and security of human lives and must comply with Federal information assurance requirements like FISMA, DHS-4300, CJIS or DIACAP.

Taking a fresh look at security is critical as agencies transition from analog voice radio to IP-based digital wireless. Any type of network is vulnerable to accidental or deliberate acts that could interrupt service, breach confidential information, or compromise data integrity. With an ever increasing reliance on IP-based technologies and budgetary constraints driving consolidation, the risks are now more prevalent. To protect your IP network, you must consider technologies that were probably not on your wireless horizon just a few years ago: firewalls, intrusion detection, anti-virus, router encryption and more. The risks to your operations are not just technical. Operational and managerial gaps are tied to technical vulnerabilities and account for some of the of risks in organizations.

Motorola's ASTRO®25 IP solutions are designed with information assurance in mind. They offer state-of-the-art features that enable you to enhance your security posture by preventing, detecting and responding to external and internal risks. Network security and data protection services are available to mitigate your risks pertaining to security incidents and compliance mandates. Turn to Motorola for assistance in assessing your security needs and configuring your new or existing ASTRO 25 network so that your personnel can continue to depend on the confidentiality, integrity, and availability of their communications.

What is Information Assurance?

Information Assurance (IA) is a combination of technologies and processes that manage information-related risks. The goal of IA is to ensure that your networks deliver:

Confidentiality: No one can obtain information from your network without proper authorization

Integrity: Stored and transmitted information (both voice and data) is protected against errors, unauthorized deletions and deliberate tampering

Availability: The network performs reliably, delivering services to users whenever requested

For government agencies an immediate concern is complying with locally-relevant IA regulations and legal requirements. Even if your IT resources are limited, Motorola can help you develop an IA program that optimizes your ASTRO 25 network's operational resilience while establishing the policies, procedures, processes, internal standards and security controls to comply with IA requirements.

How do you achieve it?

Three tasks are paramount to protecting your data, IP networks, and IT infrastructure:

Prevention: Access control mechanisms defend the system against threats and vulnerabilities. The mechanisms can be as basic as a padlock on the equipment room door, or as complex as firewall protection, digital encryption, or biometric scanners that authenticate fingerprints before allowing a user to operate a radio or gain access to a dispatch center.

Detection: Potentially significant events, such as repeated failed attempts at user log-in, must be recognized, documented, and saved for later analysis. Events that require immediate response might trigger alerts on a network administrator's screen or activate a technician's pager.

Response: Any security breaches that occur must be quickly mitigated, isolated, and prevented from happening again. Damaged or compromised systems must be swiftly restored to ensure system availability because human lives depend on it.

As a major stakeholder in public safety and critical infrastructure, Motorola is fully committed to IA programs and a defense-in-depth security architecture that guards against external and internal threats. Motorola understands the requirements for mission-critical secure systems and has the technology and services to support your IA initiatives today and into the future.

Best Practices for IP Network Security

Protect your communications and ensure compliance by taking full advantage of the security functions that can be activated on your ASTRO 25 system.

Master Site Security

Secure the heart of your ASTRO 25 network with a range of security features that could include:

Central authentication: The authentication process manages the unique identification of site administrative users and authenticates logins by password, fingerprint, voiceprint or PIN.

Event logging: The system detects suspicious events such as login failures, changes made to hardware and software, and failures in security elements. Information about these events is recorded on a central server so it can be easily retrieved and analyzed, helping network technicians promptly detect, diagnose, and respond to possible security breaches.

Backup and recovery: A backup server stores the network's volatile data (configuration files, log data, etc.) so this information can be quickly recovered in the event of hardware failure, software problems, or data loss events to get your network running again.

Element and operating system hardening: Motorola's element and operating system hardening services meet NIST & DISA guidelines. Element hardening prevents unauthorized access by identifying, monitoring, and resolving known vulnerabilities. Hardening of the operating system disables unnecessary services, hardens system passwords, and prevents unauthorized intrusions.

Zone core protection: Prevents exposure of zone core to undesirable network traffic. Detects unauthorized packets entering the zone core. Responds to unauthorized access by notifying user/system and logging event. Thus, extending the Perimeter Security solution to the network's remote site connections

Remote Site Security

Protect information as it travels across your network sites by implementing features like:

Router encryption: Safeguard information against unauthorized interception as it moves between radios, dispatch, management, and master sites. Network-layer packet encryption provides an extra layer of security to protect packets that may have to travel across public network circuits. This important feature complies with FIPS 140-2. NIAP certification to Common Criteria EAL 4 is in progress.

Port security: To prevent unauthorized devices from network access, network ports may be configured in one of three states: MAC Port Locked – only the device with the correct MAC address may connect to this port, 802.1x – connections made to this port must be authenticated, or disabled – no devices can connect to this port.

Router Access Control Lists (ACL): ACLs prevent unauthorized traffic from crossing network boundaries, thus ensuring that only allowed traffic can traverse the network. ACLs are configured based on federal standards.

Secure Shell (SSH): Authorized personnel may safely log in from any location to perform maintenance tasks and monitor key system parameters. The SSH, authenticates remote sessions and encrypts session traffic, thus preventing the unauthorized monitoring of administrative traffic.

SNMP v3: IT professionals have been using the Simple Network Management Protocol (SNMP) for years. Within the ASTRO 25 network, the newest version of this protocol (v3) delivers robust protection from unauthorized interception or modification for critical messaging between remote sites and the network fault management tools. SNMP v3 enables message integrity checking, message authentication and message encryption.

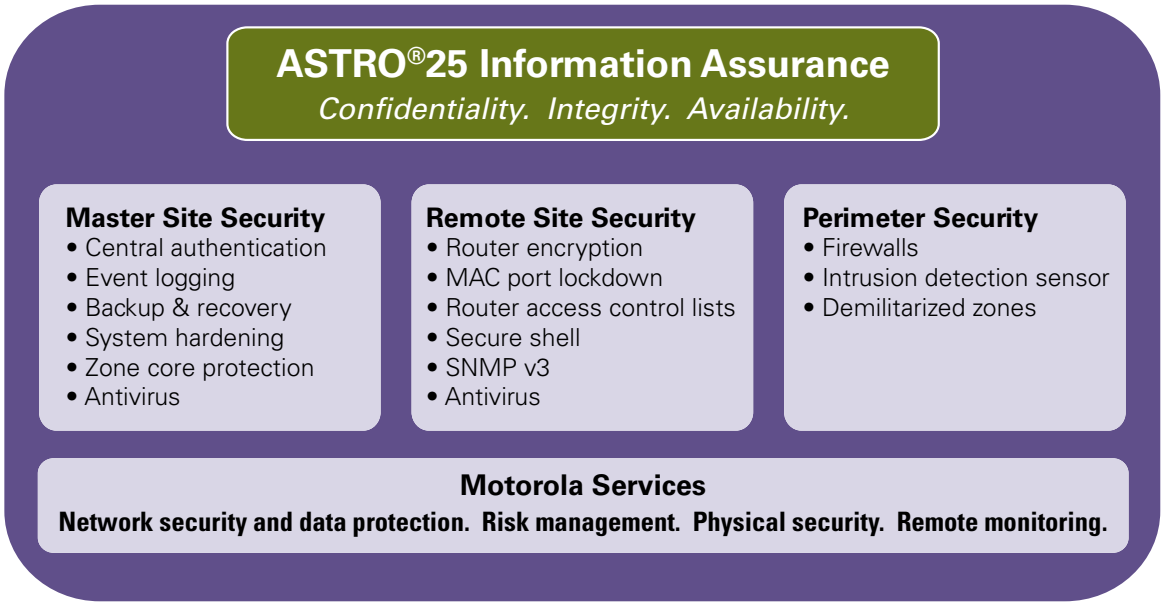
Perimeter Security

Defend your network against outside attacks using any combination of these features:

Firewalls: Firewalls inspect incoming packets and permit only valid, identified land mobile radio (LMR), dispatch, mobile data and support traffic to traverse your network.

Intrusion Detection Sensor (IDS): Detect unauthorized traffic attempting to pass through the firewall. The IDS looks for patterns that are known to be attempted intrusions and generates logs of suspicious activities.

Demilitarized Zones (DMZ): Create a buffer between enterprise and radio networks.



Motorola Security Services

Motorola experts can assist you in developing an IA strategy that works within your current resources, complies with Federal and local requirements, and supports your personnel with reliable communications on the job.

Security Services

Motorola's Security Assessment Services provide an in-depth evaluation to ensure that your wired and wireless networks are properly configured and secured according to industry best practices. The findings serve as a roadmap for mitigating technology and operational risks. Depending on your needs, the assessment may cover:

- Onsite security assessments of LMR network and related IP and wireless LAN/WAN
- Infrastructure, including physical network assets and facilities
- Design of defense-in-depth threat protection systems for IP wired and wireless networks
- Interface of ASTRO 25 networks to enterprise IP infrastructure
- Policy design, incident response planning and risk management
- Regulatory compliance strategies

Risk Management Services

Overlook a threat to the networks and you may be exposed to downtime or security breaches. Overprotect, and you may be wasting resources. Motorola's Risk Management team can help you understand and prioritize vulnerabilities so you can invest accordingly.

Physical Security Services

From natural disaster to criminal action, physical threats can disrupt your communications. Motorola's industry-leading experts have extensive backgrounds in physical security and law enforcement. They can assess your security procedures and evaluate your controls, alarm systems, electronic surveillance measures, and personnel response policies. Then they can recommend a course of action to improve your overall security posture.

24x7 Network Security Monitoring

Motorola's Managed Security Services team, working from our Secure Operations Center (SOC), provides 24x7 monitoring of network performance, firewalls and intrusion detection to help secure your communications and information systems. Motorola's SOC is a secure support environment in accordance with the Federal U.S. Government's mandated security requirements.

Pre-Tested Software Subscription (PTSS)

Obtain security updates for anti-virus definitions, intrusion detection, and operating system patches. The PTSS allows you to safely implement updates and tests for anomalies while the system continues its regular operations, making it a cost-effective service that expedites network element patching while keeping your security software up to date.

Information Assurance is all about confidence: Trust a vendor who understands what it means to be mission critical

With 75+ years of experience in working with public safety and government agencies, Motorola is a leading provider of mission critical network infrastructure. We know that our customers are counting on their communications when reputations, budgets and lives are on the line. Customers look to us for:

- Solutions that deliver real-time information into the hands of first responders –because better information leads to better decisions and better outcomes
- An established track record of delivery, design and implementation of wwcomplex technologies from a proven, long-term partner
- Seamless connectivity across multiple mission critical voice, broadband data and public networks
- Our comprehensive MOTOA4 portfolio of easy-to-use applications, ergonomically-designed equipment, and fully integrated solutions designed from the ground up to meet the special needs of public safety, first responders, government agencies, and the military
- Secure, dependable solutions and a suite of support services to enable Information Assurance at every stage in the network's life cycle

U.S. Department of Defense Requirements:

The U.S. Federal Government and military branches require compliance to security standards for all operational IP networks. Consequently, IP network infrastructures that support LMR operations must comply with FISMA/NIST, DISA, DHS-4300, and/or DITSCAP/DIACAP standards and receive certification.

Motorola ASTRO25 solutions are designed to enable compliance with these requirements while being aware of your budgetary constraints.

CJIS: Criminal Justice Information System

DIACAP: Department of Defense Information Assurance Certification and Accreditation Process. Provides a set of requirements for connection to DoD and other federal systems, networks and applications.

DISA: Defense Information Systems Agency

DITSCAP: Department of Defense Information Technology Security Certification and Accreditation Process

FIPS: Federal Information Processing Standards

FISMA: Federal Information Security Mandate Act

NIST: National Institute of Standards and Technology

NIST-FIPS800: a process to identify security risks and vulnerabilities that is required by most Federal Agencies for themselves and their subcontractors.

MOTOA4™

MOTOA4™ Mission Critical Portfolio

The ASTRO 25 network is part of the MOTOA4 Mission Critical Portfolio that offer seamless connectivity between first responders. Motorola puts real-time information in the hands of public safety and government personnel to provide better information that enables better decisions for better outcomes. It's Technology That's Second Nature.

For more information about Information Assurance for ASTRO 25 networks and the entire MOTOA4 mission critical portfolio, please visit our website or contact your Motorola representative.

motorola.com/secondnature

MOTOROLA

Motorola, Inc.
1301 E. Algonquin Road
Schaumburg, Illinois 60196 U.S.A.
www.motorola.com/secondnature
1-800-367-2346

RO-99-2172