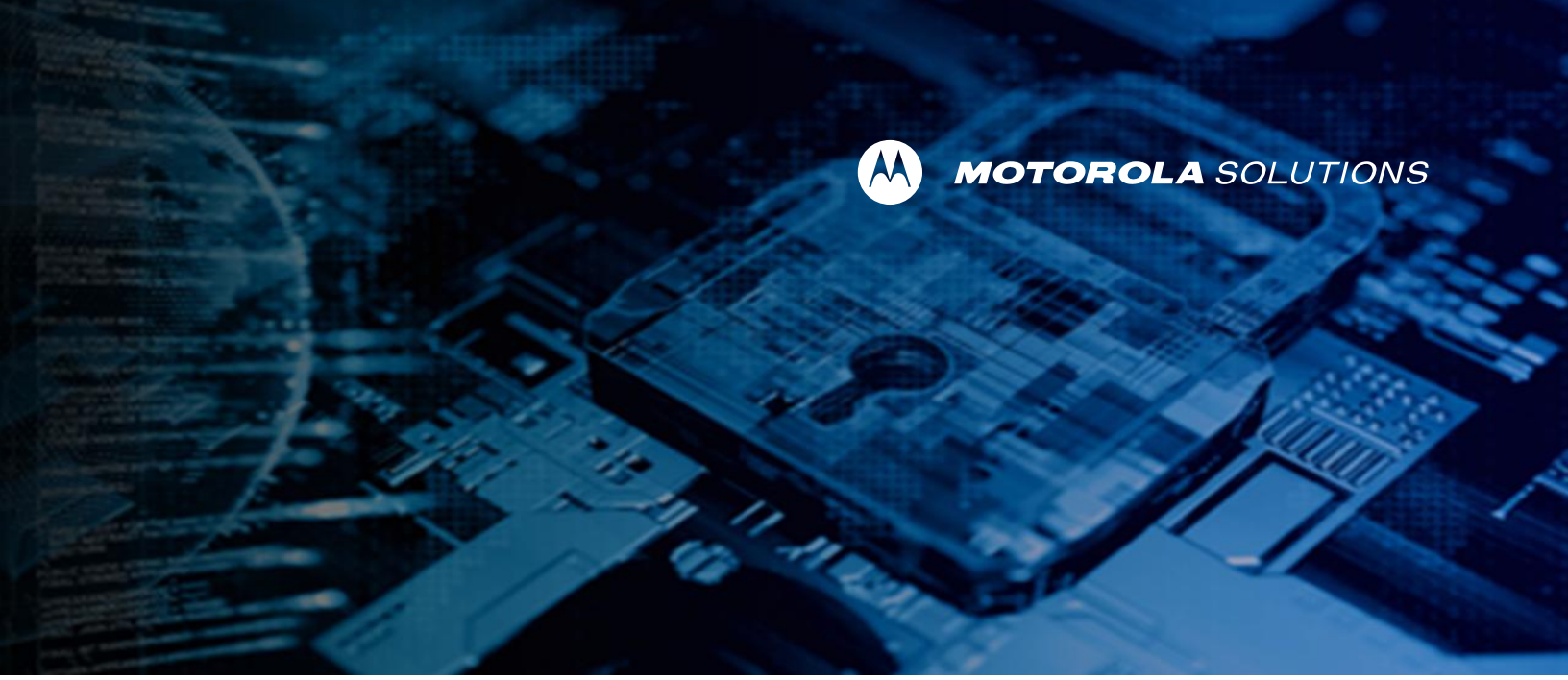

Burleson, City of

ASTRO® 25 Advanced Services Statement of Work

USC000015694

Table of Contents

Section 1

Overview

Motorola Solutions, Inc.'s (Motorola) ASTRO® 25 Advanced Services (Advanced Services) provide an integrated and comprehensive sustainment program for fixed end network infrastructure equipment located at the network core, RF sites, and dispatch sites. Advanced Services do not include maintenance for mobile devices, portable devices, or network backhaul equipment.

Advanced Services consist of the following elements:

- ASTRO System Monitoring
  - Managed Detection and Response (MDR)
  - Network Event Monitoring
  - ASTRO Connectivity Service (ACS) enabled for RSUS, System Monitoring
- Remote Technical Support
- Network Hardware Repair
- Security Update Service (SUS)
- Remote Security Update Service (RSUS)
- On-Site Infrastructure Response
- Annual Preventative Maintenance

Each of these elements is summarized below and expanded upon in Section 4: Advanced Services Detailed Description. In the event of a conflict between the descriptions below and an individual subsection of Section 4: Advanced Services Detailed Description, the individual subsection prevails.

This Statement of Work (SOW), including all of its subsections and attachments is an integral part of the applicable agreement (Agreement) between Motorola and the customer (Customer).

Notwithstanding, the connectivity contemplated in the ASTRO 25 Connectivity Service will be provided by Motorola Solutions Connectivity Inc., a wholly owned subsidiary of Motorola. In order to enable delivery of these connectivity services, customers must sign the Transport Connectivity Addendum (TCA) attached to the Agreement. Any transport or connectivity will be provided by Motorola Solutions Connectivity, Inc.

Motorola Solutions Connectivity, Inc. will utilize Motorola as its billing and collection agent and Customer expressly agrees that invoices for services provided by Motorola Solutions Connectivity, Inc. may appear on invoices issued by Motorola. Charges for Motorola Solutions Connectivity, Inc. services that appear on invoices issued by Motorola shall be paid to Motorola and are fully satisfied under the billing and payment terms of the Agreement.

In order to receive the services as defined within this SOW, the Customer is required to keep the ASTRO 25 system within a standard support period as described in Motorola's Software Support Policy (SwSP).

ASTRO System Monitoring

ASTRO System Monitoring Service includes advanced network and security monitoring along with connectivity to deliver these services.

- Managed Detection and Response

Experienced, specialized cybersecurity analyst at Motorola's Security Operations Center (SOC) will monitor the Customer's ASTRO 25 radio network for security threats. SOC analysts will coordinate with the Customer through the ActiveEye™ Security Platform to identify and mitigate threats to the Customer's networks.

- Network Event Monitoring

Real-time, continuous ASTRO 25 radio communications network monitoring and event management. Using sophisticated tools for remote monitoring and event characterization, Motorola will assess events, determine the appropriate response, and initiate that response. Possible responses include remotely addressing the issue, escalation to product technical support groups, and dispatch of designated field technical resources.

- ASTRO Connectivity Service

The highly scalable ASTRO Connectivity Service provides simple, secure link connections for the services outlined in this SOW. Motorola Solutions Operation Centers internally monitor the link's performance to ensure smooth operations to deliver the above mentioned services.

Remote Technical Support

Motorola will provide telephone consultation with specialists skilled at diagnosing and swiftly resolving infrastructure operational technical issues that require a high level of ASTRO 25 network experience and troubleshooting capabilities.

Network Hardware Repair

Motorola will repair Motorola-manufactured infrastructure equipment and select third-party manufactured infrastructure equipment supplied by Motorola. Motorola coordinates the equipment repair logistics process.

Security Update Service

Motorola will pretest third-party security updates to verify they are compatible with the ASTRO 25 network. Once tested, Motorola posts the updates to a secured extranet website, along with any recommended configuration changes, warnings, or workarounds.

Remote Security Update Service

Motorola will pre-test third-party security updates to verify they are compatible with the ASTRO 25 network, and remotely push the updates to the Customer's network.

On-Site Infrastructure Response

When needed to resolve equipment malfunctions, Motorola will dispatch qualified local technicians to the Customer's location to diagnose and restore the communications network. Technicians will perform diagnostics on impacted hardware and replace defective components. The service technician's response time will be based on pre-defined incident priority levels.

Annual Preventive Maintenance

Qualified field service technicians will perform regularly scheduled operational testing and alignment of infrastructure and network components to verify those components comply with the original manufacturer's specifications.

Section 2

Motorola Service Delivery Ecosystem

Advanced Services are delivered through a tailored combination of local field service personnel, centralized teams equipped with a sophisticated service delivery platform, product repair depots and Customer Hub. These service entities will collaborate to swiftly analyze issues, accurately diagnose root causes and promptly resolve issues to restore the Customer's network to normal operations.

2.1 Centralized Managed Support Operations

The cornerstone of Motorola's support process is the Centralized Managed Support Operations (CMSO) organization, which includes the Service Desk and technical support teams. The CMSO is staffed 24/7 by experienced personnel, including service desk specialists, security analysts and operations managers.

The Service Desk provides a single point of contact for all service related items, including communications between the Customer, Motorola, and third-party subcontractors. The Service Desk processes service requests, service incidents, change requests, and dispatching, and communicates with stakeholders in accordance with predefined response times.

All incoming transactions through the Service Desk are recorded, tracked, and updated through the Motorola Customer Relationship Management (CRM) system. The Service Desk also documents Customer inquiries, requests, concerns, and related tickets.

The CMSO coordinates with the field service organization that will serve the Customer locally.

2.2 Field Service

Motorola authorized and qualified field service technicians perform on-site infrastructure response, field repair, and preventive maintenance tasks. These technicians are integrated with the Service Desk and with technical support teams and product engineering as required to resolve repair and maintenance requests.

2.3 Customer Support Manager

A Motorola Customer Support Manager (CSM) will be the Customer's key point of contact for defining and administering services. The CSM's initial responsibility is to create the Customer Support Plan (CSP) in collaboration with the Customer.

The CSP functions as an operating document that personalizes the services described in this document. The CSP contains Customer-specific information, such as site names, site access directions, key contact persons, incident handling instructions, and escalation paths for special issues.

The CSP also defines the division of responsibilities between the Customer and Motorola so response protocols are pre-defined and well understood when the need arises.

The CSP governs how the services will be performed and will be automatically integrated into this SOW by this reference. The CSM and Customer will review and amend the CSP on a mutually agreed cadence so the CSP remains current and effective in governing the Advanced Services.

2.4 Customer Hub

Supplementing the CSM and the Service Desk as the Customer points of contact, Customer Hub is a web-based platform that provides network maintenance and operations information. The portal is accessed from a desktop, laptop, tablet or smartphone web browser. The information available includes:

- **Network Event Monitoring**: Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.
- **Remote Technical Support**: Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.
- **Network Hardware Repair**: Track return material authorizations (RMA) shipped to Motorola's repair depot and eliminate the need to call for status updates. In certain countries, customers will also have the ability to create new RMA requests online.
- **On-Site Infrastructure Response**: Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.
- **Annual Preventive Maintenance**: View incident status and details of each annual change request for preventive maintenance, including completed checklist information for the incident.
- **Network Updates**: View system status overview and software update information.
- **Managed Detection and Response**: Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.
- **Orders and Contract Information**: View available information regarding orders, service contracts, and service coverage details.

The data presented in Customer Hub is provided to support the services described in the following sections, which define the terms of any service delivery commitments associated with this data.

Section 3

Connectivity Specifications

A monitored access link is provided via the ASTRO Connectivity Service with bandwidth necessary to support the services included in this SOW.

Section 4

Advanced Services Detailed Description

Due to the interdependence between deliverables within the detailed sections, any changes to or any cancellation of any individual section may require a scope review and price revision.

4.1 ASTRO System Monitoring (NEW)

4.1.1 Managed Detection and Response

Motorola Solutions, Inc. (Motorola) ASTRO® 25 Managed Detection and Response (MDR) provides monitoring of radio network security information by specialized cybersecurity analysts with extensive experience working with ASTRO 25 mission-critical networks.

The following sections describe the deliverables of the service, its technologies, and service obligations.

This Statement of Work (SOW), including all of its subsections and attachments, is an integral part of the applicable agreement (Agreement) between Motorola and the Customer.

In order to receive the services as defined within this SOW, the Customer is required to keep the system within a standard support period as described in Motorola's Software Support Policy (SwSP).

4.1.1.1 Description of Service

MDR is performed by Motorola's Security Operations Center (SOC) using the ActiveEye℠ security platform. The SOC cybersecurity analysts monitor for alerts 24/7. If a threat is detected, analysts will investigate and initiate an appropriate Customer engagement. Customer engagements may include, but are not limited to, deploying cybersecurity countermeasures for incident containment, requesting additional information from the Customer, continuing to monitor the event for further development, or informing the Customer to enact the Customer's documented Incident Response Plan.

SOC analysts rely on monitoring elements to detect signs of a potential threat impacting the Customer's ASTRO 25 network and applicable Customer Enterprise Network (CEN) systems. These elements are described below.

The MDR service includes the deployment and optimization of these elements into the Customer's network.

4.1.1.2 Managed Detection and Response Elements

This section and its subsections describe MDR elements, and their applicability for specific infrastructure.

ActiveEye Security Platform

Motorola's ActiveEye security platform collects and analyzes security event streams from Endpoint Detection and Response, EDR, agents and embedded ActiveEye Remote Security Sensors (AERSS) in the Customer's ASTRO 25 network and applicable CEN systems, using security orchestration and advanced analytics to identify the most important security events from applicable systems. The ActiveEye platform is provided in the English language.

The platform automates manual investigation tasks, verifies activity with external threat intelligence sources, and learns what events will require rapid response action.

The Customer will receive access to the ActiveEye platform as part of this service. ActiveEye will serve as a single interface to display system security information. Using ActiveEye, the Customer will be able to configure alerts and notifications, review security data, and perform security investigations.

Applies to included ASTRO 25 Radio Network Infrastructure (RNI), CEN, and Control Room CEN infrastructure.

ActiveEye Remote Security Sensor

One or more AERSS will be deployed into the ASTRO 25 network and if applicable to CEN environments to deliver the service. These sensors monitor geo diverse sites for security events and pass security information to the ActiveEye platform.

AERSS integrate the ActiveEye platform with network elements, enabling it to collect logs from Syslog, as well as to analyze network traffic over monitor ports and scan elements for vulnerabilities.

The following are the environmental requirements and specifications the Customer must provide to prepare for the AERSS deployment.

Specification	Requirement
Rack Space	1U
Power Consumption (Max)	550 Watts (Redundant Power Supply
Power Input	100-240V AC
Current	3.7 A – 7.4 A
Circuit Breaker	Qty. 2
Line Cord	NEMA 5-15P
Heat Dissipation (max)	2107 BTU/hr.

Applies to included ASTRO 25 RNI, CEN, and Control Room CEN infrastructure.

Endpoint Detection and Response

Endpoint Detection and Response (EDR) is an endpoint security agent that integrates with the ActiveEye security platform to provide additional threat detection, investigation, and response actions to optimize protection of critical systems.

EDR integration with ActiveEye accelerates investigations by making necessary information available for analysts in a single platform where they can quickly access details of what caused an alert, its context, and its history.

The platform enables analysts to initiate response actions (i.e. isolate host, ban or block a file hash, terminate a process) on endpoints to respond to detection of verified malicious activity within the system. Available responses are determined by the Customer's security policies.

Cloud Based Vulnerability Scan Engine

Cloud based scan engines probe internet facing assets such as firewalls and VPNs to identify unpatched vulnerabilities and insecure configurations.

Scan findings are published as reports in the ActiveEye security platform.

Control Room Firewall

In cases where an ASTRO 25 site (Network Management Dispatch, Trunking Subsystem, Conventional Subsystem) has insufficient bandwidth to support EDR communications, an optional Control Room Firewall can be integrated at the site. When this is done, EDR communications will be configured to leverage that firewall in place of the site link. This configuration will not change any existing traffic flows in the system that currently leverage the site link.

The following are the environmental requirements and specifications the Customer must provide to prepare for the Control Room Firewall deployment.

Specification	Requirement
Rack Space	1U
Power Consumption (Max)	28.6 W (Single Power Supply)
Power Input	100-240V AC
Current	.52 A
Circuits Breaker	Qty. 1
Heat Dissipation (Max)	97.6 BTU/hr
Line Cord	NEMA 5-15P
Internet Service Bandwidth	High availability Internet Connection (99.99% [4-9s] or higher) Packet loss < 0.5% Jitter < 10 ms Delay < 120 ms RJ45 Port Speed – Auto Negotiate

Applies to included ASTRO 25 RNI, CEN, and Control Room CEN infrastructure.

Internetworking Firewall

Motorola introduces a formalized and centralized Internet connection to the ASTRO 25 system using an Internetworking Firewall.

The Internetworking Firewall serves as a security barrier and demarcation point between a master site and the Internet (or a customer network leading to the Internet). The Internetworking Firewall supports traffic for various ASTRO 25 features that require access to the Internet.

The Internetworking Firewall sits between the Demilitarized Zone (DMZ) and the Internet (or customer network leading to the Internet).

The following are the environmental requirements and specifications the Customer must provide to prepare for the Internetworking Firewall deployment.

Specification	Requirement
Rack Space	1U
Power Consumption (Max)	28.6 W (Single Power Supply)
Power Input	100-240V AC
Current	.52 A
Circuits Breaker	Qty. 1
Heat Dissipation (Max)	97.6 BTU/hr.
Line Cord	NEMA 5-15P
Internet Service Bandwidth	Bandwidth throughput 10 Mbps per AERRS High availability Internet Connection (99.99% (4-9s) or higher). Packet loss < 0.5%. Jitter <10 ms. Delay < 120 ms. RJ45 Port Speed - Auto Negotiate

4.1.1.3 Deployment Timeline and Milestones

The following phase descriptions lay out the necessary deployment activities and milestones required to achieve service readiness:

Phase 1: Service Onboarding

After contract signature, Motorola will schedule a service kickoff meeting with the Customer and provide information-gathering documents. This kickoff meeting is conducted remotely at the earliest, mutually available opportunity within 30 days of contract signing (Kickoff Date). Customer is to identify and ensure participation of key team members in kickoff and project initiation activities.

On the Kickoff Date, the Customer will be provisioned onto the ActiveEye MDR portal. The portal will enable service notifications, access to vulnerability scans and cybersecurity advisories. The first vulnerability scan will be conducted and reported within 30 days following the Kickoff Date. On the Kickoff Date, the Customer will receive instructions for accessing the Security Operations Center and Incident Response (IR) teams. Once access is provisioned, the Customer will receive any assistance required from the IR team and be able to configure key contacts for interaction with the Security Operations team. The Customer will receive instructions for accessing the Security Operations Center within the first 30 days.

Phase 2: Infrastructure Readiness

Motorola will provide detailed requirements regarding Customer infrastructure preparation actions at the kickoff meeting. It is the Customer's responsibility to accomplish all agreed upon infrastructure preparations. It is Motorola's responsibility to separately complete any obligated and/or agreed infrastructure readiness tasks.

Phase 3: System Buildout and Deployment

Motorola will build and provision tools in accordance with the requirements of this proposal and consistent with information gathered in earlier phases. Motorola will also provide detailed requirements regarding Customer deployment actions. The Customer may be required to deploy software and/or configurations in cases where Motorola does not manage the device and does not have access or authorization to perform the installation.

Motorola will coordinate with the customer to identify and schedule mutually agreeable maintenance windows where Motorola will perform integration of endpoint detection and response agents at in-scope sites and Customer Enterprise Networks (CENs). Endpoint detection and response agents will not be installed at sites that do not meet the minimum connectivity requirements (either site links with sufficient bandwidth or Control Room Firewalls with customer provided internet). Motorola will leave the existing antivirus solution in place on endpoints located at these out of scope sites.

Phase 4: Monitoring “Turn Up”

Motorola will verify in-scope assets are forwarding logs or events. Motorola will notify the Customer of any exceptions. Motorola will begin monitoring connected in-scope sources after the initial tuning period.

Phase 5: Tuning and Customer Training

Motorola will conduct initial tuning of events and alarms in the service, and conduct an additional ActiveEye Portal training session.

Service Commencement

The Service will commence with the Service Onboarding phase or within 30 days of contract signature, whichever event occurs soonest for existing customers.

In the case of a new ASTRO system, the Service will commence in parallel to the commencement date of the core ASTRO Service package “Turn Up" go live date. Motorola and the Customer will collaborate to complete the additional deployment tasks.

4.1.1.4 General Responsibilities

Motorola Responsibilities

- Provide and when necessary repair under manufacturer warranty hardware and software required to remotely monitor the ASTRO 25 network and applicable CEN systems inclusive of the AERSS and all software operating on it.
  - If the Centralized Event Logging feature is not installed on the Customer’s ASTRO 25 RNI, Motorola will install it as part of this service.
- Coordinate with the Customer on any system changes necessary to integrate the AERSS into the system and establish necessary connectivity.
- Provide software and licenses to the Customer necessary to remotely monitor the ASTRO 25 network and applicable CEN environments.
- Integrate EDR agents as per the “Deployment Timeline and Milestones” section in all network segments where endpoint detection and response is in scope.
  - Note that network segments with insufficient connectivity to support endpoint detection and response will be considered out of scope for endpoint detection and response

  - Motorola will perform the installation of endpoint detection and response agents in the RNI-DMZ CEN(s) and Control Room CEN(s) for all Motorola managed devices that support endpoint detection and response agents.
  - Motorola will support the customer with installing endpoint detection and response agents in the RNI-DMZ CEN(s) and Control Room CEN(s) for any device that supports endpoint detection and response agents and is not Motorola Solutions managed. Due to the fact that Motorola does not typically manage the devices and network connectivity for endpoints in the Control Room CEN, it is ultimately the customer's responsibility to perform this installation.
- Assist the Customer with the installation of log forwarding agents on systems that are not managed by Motorola. Note, Motorola will perform installation on all endpoints that are managed by Motorola.
- Verify connectivity and monitoring is active prior to start of service.
- Coordinate with the Customer to maintain Motorola service authentication credentials.
- Monitor the Customer's ASTRO 25 network and applicable CEN systems 24/7 for malicious or unusual activity, using trained and accredited technicians.
- Respond to security incidents in the Customer's system in accordance with Section 1.3.6: Managed Detection and Response Priority Level Definitions and Response Times. Response may include, but is not limited to, requesting additional information from the Customer, continuing to monitor the event for further development or informing the Customer to enact the Customer's documented Incident Response plan.
- Assist the Customer with identifying devices that support logging within the ASTRO 25 network and applicable CEN systems have been configured to forward Syslog events to the AERSS.
- Provide the Customer with access to the ActiveEye platform enabling Customer access to security event and incident details.

Customer Responsibilities

- The ASTRO 25 MDR service requires a connection from the Customer's ASTRO 25 network and applicable CEN systems to the Internet. Establish connectivity with sufficient bandwidth before the service commences. Internet service bandwidth requirements are as follows:
  - Bandwidth throughput 10 Mbps per AERSS.
  - High availability Internet Connection (99.99% (4-9s) or higher).
  - Packet loss < 0.5%.
  - Jitter <10 ms.
  - Delay < 120 ms.
  - RJ45 Port Speed - Auto Negotiate.
  - If an ASTRO site link will be leveraged for endpoint detection and response communications, that site link must support a minimum of 2 Mbps of bandwidth.
- It is the Customer's responsibility or the contracted maintainer to install the AERSS device in the Control Room CEN.
- Allow Motorola continuous remote access to monitor the ASTRO 25 network and applicable CEN systems. This includes keeping the connection active, providing passwords, and working with Motorola to understand and maintain administration privileges.
- Maintain an active subscription for:

  - Security Update Service (SUS) (or Remote Security Update Service), ensuring patches and antivirus definitions are applied according to the release cadence of the service.
  - ASTRO Dispatch Service and ASTRO Infrastructure Response.
  - The ASTRO 25 Managed Detection and Response service requires an ASTRO 25 WAVE SUS subscription.
- Provide continuous utility services to any equipment installed or utilized at the Customer's premises to support service delivery and remote monitoring.
- Provide Motorola with contact information necessary to complete the Customer Support Plan (CSP). Notify the Customer's Customer Support Manager (CSM) within two weeks of any contact information changes.
- Notify Motorola if any components are added to or removed from the environment as it may be necessary to update or incorporate in MDR. Changes to monitored components may result in changes to the pricing of the MDR service.
- **Ensure that the ASTRO 25 system is operating on a Motorola supported release.**
- Allow Motorola dispatched field service technicians physical access to monitoring hardware when required.
- Cooperate with Motorola and perform all acts that are required to enable Motorola to provide the services described in this SOW.
- Configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a ports on a switch) network traffic to the ActiveEye sensor for applicable CEN systems.
- Responding to Cybersecurity Incident Cases created by the Motorola SOC.

4.1.1.5 Service Modules

4.1.1.5.1 Log Collection / Analytics

The AERSS deployed in the system collects logs and other security information from applicable servers, workstations, switches, routers, network intrusion detection sensors, and firewalls. This information is forwarded to the ActiveEye platform, which uses advanced analytics to identify signs of security incidents. If it identifies signs of a security incident, ActiveEye notifies the SOC for further analysis.

Motorola Responsibilities

- Consult with and advise the Customer on performing necessary system configurations to direct log sources to the appropriate Remote Security Sensor.
- The SOC will consult with the Customer to identify appropriate log sources for the level of threat detection desired in each environment.

Customer Responsibilities

- If applicable, configure customer managed networking infrastructure to allow AERSS to communicate with ActiveEye as defined.
- If applicable, configure any Customer managed devices in the CEN to forward data to ActiveEye.

Applies to included ASTRO 25 RNI, CEN, and Control Room CEN infrastructure.

4.1.1.5.2 Network Detection

The AERSS deploys a Network Intrusion Detection System (NIDS), constantly monitoring traffic passing across, into, or out of the infrastructure. Network Detection analyzes traffic for signs of malicious activity in real time, and performs packet level and flow level analysis to enable communications modeling. This information is used to identify anomalous behavior that is not captured by pre-defined traffic signatures, including traffic using encrypted connections. Network Detection alerts the SOC for further analysis.

Motorola Responsibilities

- Work with the Customer to integrate AERSS.
- Optimize the policies and configuration to tune out noise and highlight potential threats.
- The SOC consults with the Customer to identify the appropriate deployment of Network Detection Service Components. The SOC monitors and updates the security policy of each sensor to tune out unnecessary alerting and flow monitoring so that the system is optimized to detect true malicious activity.

Customer Responsibilities

- If necessary, configure Customer's networking infrastructure to allow AERSS to communicate with ActiveEye as defined.
- For Customer's owned CEN infrastructure, configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a ports on a switch) network traffic to the ActiveEye sensor.
- Initiate recommended response actions when active attacks are detected.

Applies to included ASTRO 25 RNI, CEN, and Control Room CEN infrastructure.

4.1.1.5.3 Endpoint Detection and Response

Endpoint detection and response agents deployed on in-scope and supported Windows and Linux hosts and servers throughout the system constantly monitor for indicators of compromise and feed this information back to the ActiveEye security platform. The Security Operations Center monitors this feed and is ready 24/7 to take action when a detection is made.

Motorola Solutions Responsibilities

- Install and/or support the installation of endpoint detection and response agents on in scope endpoints in the system as detailed in the "Deployment Timeline and Milestones" section.
- Monitor endpoint detection and response feeds for detections of indicators of compromise.
- In the event of the detection of an indicator of compromise, perform detailed investigations of the event .
- Per the Customer's security policies and defined incident response plan, alert and engage the customer and potentially take an action to deploy a countermeasure to contain the incident.

Customer Responsibilities

- Work with Motorola to ensure that there is a documented incident response plan that indicates how Motorola should engage with the Customer in the event of a detection of an indicator of compromise.
- Provide and maintain contact information for a Customer point of contact that can take action or authorize Motorola to take action in the event of a detection of an indicator of compromise.

Applies to in scope ASTRO 25 RNI, CEN, and Control Room CEN infrastructure.

4.1.1.5.4 External Vulnerability Scanning

External Vulnerability Scanning is provided for the ASTRO internet-facing, external network interfaces. The scan is enabled from an internet cloud hosted service outside the ASTRO network. Discovery and vulnerability scans will be run quarterly or on a less frequent schedule defined with the Customer.

The initial scan results will be discussed with the Customer during service onboarding. Subsequent scans will be reviewed by a cybersecurity analyst. If any new findings of interest are surfaced, a ticket will be created to communicate these findings with the customer defined contacts.

Motorola Responsibilities

- Configure scans to match the Customer's preferences for external scope.
- Verify vulnerability scans are operating correctly.
- Make generated results available in the Customer's ActiveEye portal.
- Create ticket notifications for significant, new findings of interest.

Customer Responsibilities

- During Service Onboarding kickoff, provide Motorola with the IP addresses and/or domain names to be included in the external vulnerability scans.
- In accepting this Statement of Work, the Customer authorizes Motorola to engage in external vulnerability scans of internet-facing, external assets disclosed by the Customer.
- Be responsible for updating Motorola with any changes to the IP addresses and/or domain names of the internet-facing, external assets subject to the external vulnerability scans.
- If the information required to enable vulnerability scanning of the internet-facing, external assets is not provided initially or is not current at any time during the term, Motorola will suspend scans until it is reasonably satisfied that it has been provided with the most current information.
- Review all quarterly vulnerability reports, and tickets of new findings.
- Perform any remediation actions required to address identified vulnerabilities.

Applies to Internet facing assets only.

4.1.1.5.5 Advanced Threat Insights

With Advanced Threat Insights, Motorola provides continuous dark web monitoring, alerts and notifications, customer risk reviews, organization-specific threat intelligence and industry-level threat intelligence. Trained cybersecurity analysts will search the dark web looking for indications that any of the Customer's systems, customer user accounts in the monitored domain, or data sets have been

compromised. In addition, cybersecurity analysts will search for evidence that the Customer's organization or primary applications may be the target of a threat actor campaign.

Motorola's cybersecurity analysts will develop threat reports and review them with the Customer. Analysts perform threat intelligence gathering using a combination of automated and human methods. They review threat intelligence findings during normal US business hours 8x5 on standard U.S. business days: Monday through Friday 8 a.m. to 5 p.m. local time, excluding U.S. holidays.

There are four main aspects of this service:

- Named Analyst - A dedicated analyst will work with the Customer to understand the organization's operating environment and architecture in more detail and depth. This approach enables the analyst to provide detailed recommendations for improving the Customer's overall risk posture from a consistent single point of contact.
- Proactive Threat Hunting - The analyst will dedicate time each month (number of hours dependent on subscription) to evaluate available threat intelligence and sensor information (log analysis, NIDs, etc.) to identify areas of concern. This manual investigation can uncover previously undetected threats that exist outside of the scope of typical security alerting and provide a starting point for remediation and security recommendations to improve the Customer's overall security posture. The focus of this work can be directed by the customer toward the most critical assets or those assets most at risk given the threat landscape at the time.
- Surface, Deep, and Dark Web Insights - Risks go beyond the visible boundaries of the organization. Monitoring for key assets on the surface, deep, and dark web provides actionable insights into how the organization is being targeted and what assets are at risk, such as lost or exposed credentials and sensitive data.
- Monthly Summary and Discussion of Findings - The assigned analyst will present key findings for the past month, discuss new threats to consider, and suggest any additional security measures relevant to the Customer's organization.

Motorola Responsibilities

- Coordinate with the Customer to collect relevant information necessary to complete threat intelligence searches on the dark web.
- Deliver a monthly risk report detailing threat intelligence specific to the Customer.
- Provide the Customer with a monthly public safety industry intelligence report detailing threat intelligence related to the public safety community as a whole.
- Hold recurring formal risk reviews with the Customer to evaluate threats facing the Customer and intelligence discoveries. This review also serves as an opportunity to refine the list of critical information the threat team needs to proactively search for.
- Alert the Customer immediately when critical threats or information breaches are discovered.

Customer Responsibilities

- Coordinate with Motorola to maintain relevant information necessary to complete threat intelligence searches on the dark web.
- Obtain for Motorola all rights, if any, which may be necessary to permit requested threat intelligence searches on the dark web.

4.1.1.5.6 Disclaimer

Scope of services do not include employee related investigative services, such as those that may target any specific employees (or other individuals) or implicate privacy rights, alleged or suspected internal conduct, or rights that may be protected or regulated by law, e.g. information bearing on an individual's character, general reputation, personal characteristics, mode of living, etc. Motorola reserves the right to withhold from Customer any information deemed outside the scope of the engagement or otherwise subject to legal restrictions and take any other action it deems to be required by law.

Customer understands that some information shared with Customer through the Advanced Threat Insights service will, by its nature, be unverifiable, will be delivered on an as-is basis, and may or may not be correct. Customer agrees any information shared is for Customer's internal business purpose use only and shall not be further distributed by Customer.

Motorola does not represent that it will identify, fully recognize, discover, or resolve all security events or threats, system vulnerabilities, malicious codes or data, backdoors, or other system threats or incompatibilities as part of the service, or that the agreed upon cadence/time of delivery will be sufficient to identify, mitigate or prevent any cyber incident.

For subscribers of the Advanced Threat Insights service, Motorola disclaims any warranty and does not guarantee to be able to locate all threat intelligence on the surface, deep or dark web. Motorola will perform an expansive search but cannot cover every forum and information source.

4.1.1.6 Security Operations Center Monitoring and Support

4.1.1.6.1 Scope

Motorola delivers Security Operations Center (SOC) Monitoring using one or more SOC facilities. The SOC includes any centralized hardware and software used to deliver this Service and its service modules. The SOC and its centralized hardware and software are housed within an SSAE-18 compliant data center.

Motorola's SOC is staffed with security experts who will use ActiveEye security platform to monitor elements integrated by service modules. In addition, SOC staff will take advantage of their extensive experience to investigate and triage detected threats, and to recommend responses to the Customer. Depending on Customer security policies and the extent to which endpoint detection and response is deployed within the system, the SOC may take actions to deploy countermeasures in an attempt to contain a security incident. Customer support is provided in the English language.

Motorola will start monitoring the ASTRO 25 MDR service in accordance with Motorola processes and procedures after deployment, as described in Section 1.2 Deployment Timeline and Milestones.

The SOC receives system-generated alerts 24/7, and provides the Customer with a toll-free telephone number and email address for support requests, available 24/7. Support requests are stored in a ticketing system for accountability and reporting. The SOC will respond to detected events in accordance with Section 1.3.68: Incident Priority Level Definitions and Response Times.

4.1.1.6.2 Ongoing Security Operations Center Service Responsibilities

Motorola Responsibilities

If a probable security incident is detected, provide phone and email support to:

- Engage the Customer's defined Incident Response Process.
- Gather relevant information and attempt to determine the extent of compromise using existing monitoring capabilities in place as part of the ASTRO 25 MDR service.
- Analysis and support to help the Customer determine if the Customer's corrective actions are effective.
- Continuous monitoring, in parallel with analysis, to support Incident Response.

Customer Responsibilities

- Provide Motorola with accurate and up-to-date information, including the name, email, landline telephone numbers, and mobile telephone numbers for all designated, authorized Customer escalation Points of Contact (POC).
- Provide a timely response to SOC security incident tickets or investigation questions.
- Notify Motorola at least twenty four (24) hours in advance of any scheduled maintenance, network administration activity, or system administration activity that would affect Motorola's ability to perform the Managed SOC Service, as described in this SOW.

4.1.1.6.3 Technical Support

ActiveEye Security Management Technical Support provides the Customer with a toll-free telephone number and email address for ActiveEye Security Management support requests, available Monday through Friday from 8 a.m. to 7 p.m. CST.

Motorola Responsibilities

- Notify customers of any scheduled maintenance or planned outages.
- Provide technical support, security control, and service improvements related to ActiveEye.

Customer Responsibilities

- Provide sufficient information to allow Motorola technical support agents to diagnose and resolve the issue.

Limitations and Exclusions

Technical support is limited to the implementation and use of the ActiveEye platform and does not include use or implementation of third-party components.

4.1.1.6.4 Incident Response

An Indicator of Compromise (IoC) is an observable event that Motorola Security Analysts have determined will jeopardize the confidentiality, integrity, or availability of the system. Examples of IoC include ransomware or malicious use of PowerShell.

When an IoC is observed, the Motorola Security Operations team will engage with the customer to investigate the issue, determine the extent of the compromise and contain the activity to the extent possible with the Motorola security controls deployed within the environment. This expert guidance is

available upon contract signature and extends through MDR infrastructure deployment phases and the term of the contract.

When an IoC is observed by the Security Analyst, Motorola and Customer will be responsible for the tasks defined in the following subsections.

Motorola Responsibilities

- Upon the identification of an IoC, notify the Customer's documented contact and initiate the escalation plan.
- Take documented, Customer approved actions in an attempt to contain an IoC to the extent enabled via Motorola managed technology. Communicate to the Customer any additional potential containment actions and Incident Response resources that can be taken across the Customer's managed IT infrastructure.
- Perform investigation using the ActiveEye MDR integrated and enabled data sources in an initial attempt to determine the extent of an IoC.
- Document and share IoC and artifacts discovered during investigation. Motorola services exclude performing on-site data collection or official forensic capture activities on physical devices.

Customer Responsibilities

- Maintain one named Point of Contact (PoC) to coordinate regular team discussions and organize data collection and capture across the Customer and Motorola teams.
- If determined to be required by Customer, contract an Incident Response service provider to perform procedures beyond the scope of this Agreement such as forensic data capture, additional malware removal, system recovery, ransomware payment negotiation, law enforcement engagement, insurance provider communications, identify patient zero, etc.

4.1.1.6.5 Event Response and Notification

Motorola will analyze events created and/or aggregated by the Service, assess their type, and notify the Customer in accordance with the following table.

Table 4-1: Event Handling

Event Type	Details	Notification Requirement
False Positive or Benign	Any events determined by Motorola to not likely have a negative security impact on the organization.	None
Event of Interest (EOI)	Any events determined by Motorola to likely have a negative security impact on the organization.	Escalate to Customer in accordance with routine notification procedure. Escalate in accordance with urgent notification procedure when required by agreed-upon thresholds and SOC analysis. Notification procedures are included in Table 1-2.

4.1.1.6.6 Notification

Motorola will establish notification procedures with the Customer, generally categorized in accordance with the following table.

Table 4-2: Notification Procedures

Notification Procedure	Details
Routine Notification Procedure	The means, addresses, format, and desired content (within the capabilities of the installed technology) for Events of Interest (EOI). These can be formatted for automated processing, e.g., by ticketing systems.
Urgent Notification Procedure	Additional, optional means and addresses for notifications of Events of Interest that require urgent notification. These usually include telephone notifications.

Motorola will notify the Customer according to the escalation and contact procedures defined by the Customer and Motorola during the implementation process.

4.1.1.6.7 Tuning

Motorola will assess certain events to be environmental noise, potentially addressable configuration issues in the environment, or false positives. Motorola may recommend these be addressed by the Customer to preserve system and network resources.

Motorola will provide the Customer with the ability to temporarily suppress alerts reaching ActiveEye, enabling a co-managed approach to tuning and suppressing events or alarms. The SOC may permanently suppress particular alerts and alarms if not necessary for actionable threat detection.

4.1.1.6.8 Tuning Period Exception

The tuning period is considered to be the first thirty (30) days after each service module has been confirmed deployed and configured and starts receiving data. During the tuning period, Motorola may make recommendations to the Customer to adjust the configurations of their installed software so Services can be effectively delivered. Service Availability will not be applicable during the tuning period and responses or notifications may not be delivered. However, Motorola will provide responses and notifications during this period.

Motorola may continue to recommend necessary tuning changes after this period, with no impact on Service Availability.

4.1.1.7 Incident Priority Level Definitions and Response Times

Priority for alert-generated incident or Events of Interest is determined by the ActiveEye Platform analytics that process multiple incoming alert feeds, automation playbooks, and cybersecurity analyst knowledge.

Priority	Definition	Service Coverage

Priority	Definition	Service Coverage
Critical	Security incidents that have caused, or are suspected to have caused significant damage to the functionality of the Customer's ASTRO 25 system or information stored within it. Efforts to recover from the incident may be significant. Examples: Malware that is not quarantined by anti-virus. Evidence that a monitored component has communicated with suspected malicious actors.	Response provided 24 hours, 7 days a week, including United States (U.S.) public holidays.
High	Security incidents that have localized impact and may become more serious if not quickly addressed. Effort to recover from the incident may be moderate to significant. Examples: Malware that is quarantined by antivirus. Multiple behaviors observed in the system that are consistent with known attacker techniques.	Response provided 24 hours, 7 days a week, including U.S. public holidays.
Medium	Security incidents that potentially indicate an attacker is performing reconnaissance or initial attempts at accessing the system. Effort to recover from the incident may be low to moderate. Examples include: Suspected unauthorized attempts to log into user accounts. Suspected unauthorized changes to system configurations, such as firewalls or user accounts. Observed failures of security components. Informational events. User account creation or deletion. Privilege change for existing accounts.	Response provided on standard business days, Monday through Friday 8 a.m. to 5 p.m. CST/CDT, excluding U.S. public holidays.
Low	These are typically service requests from the Customer.	Response provided on standard business days, Monday through Friday 8 a.m. to 5 p.m. CST/CDT, excluding U.S. public holidays.

Response Time Goals

Priority	Response Time
Critical	An SOC Cybersecurity Analyst will make contact with the customer technical representative within one (1) hour of the request for support being logged in the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action. Continual effort will be maintained to identify the extent of the incident and provide actions for containment.
High	An SOC Cybersecurity Analyst will make contact with the customer technical representative within four (4) hours of the request for support being logged at the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action. Continual effort will be maintained to identify the extent of the incident and provide actions for containment.

Priority	Response Time
Medium	An SOC Cybersecurity Support Engineer will make contact with the customer technical representative within the next business day of the request for support being logged at the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action.
Low	An SOC Cybersecurity Support Engineer will make contact with the Customer technical representative within seven business days of the logged request for support at the issue management system.

ActiveEye Platform Availability

The platform utilizes a multi-zone architecture which can recover from failures in different data collection, enhancement, analysis, and visualization tiers. Motorola will make commercially reasonable efforts to provide monthly availability of 99.9% for the ActiveEye Platform services. Service availability is subject to limited scheduled downtime for servicing and upgrades, as well as unscheduled and unanticipated downtime resulting from circumstances or events outside of Motorola's reasonable control, such as disruptions of, or damage, to the Customer's or a third-party's information or communications systems or equipment, telecommunication circuit availability/performance between Customer sites, any on-premises core and/or between on-premises equipment and the ActiveEye Platform.

ActiveEye Remote Security Sensor (AERSS)

One or more AERSS may be deployed as part of the MDR solution. The AERSS is configured with multiple local redundancy features such as hot-swap hard disk drives in a redundant drive array configuration and dual redundant power supplies.

The AERSS and all components of ActiveEye are monitored by a dedicated Site Reliability Engineering team. In cases of hardware failure of the AERSS, Motorola will provide, subject to active service subscriptions in the Customer contract, onsite services to repair the AERSS and restore service. AERSS operation and outage troubleshooting requires network connection to the ActiveEye Platform which may be impacted by customer configuration changes, telecommunications connectivity, and/or customer network issues/outages.

4.1.1.8 Included Services

Site Information

The following quantities are included in the scope:

Site / Location	Quantity
Primary zone cores	
DSR backup cores	
Sites (NMD, T-Sub, C-Sub)	
CEN (Control Room)	
CEN (RNI-DMZ)	
Network Management Clients	

Site / Location	Quantity
Dispatch Consoles	4
AIS	1
CEN Endpoints	

Services Included

The ActiveEye service modules included in this statement of work are viewable in the Subscribed column below. The Network Environment column designates the location of each module: ASTRO 25 Radio Network Infrastructure (RNI), Customer Enterprise Network (CEN), or the Control Room CEN.

Service Module	Features Included	Network Environment	Subscribed
ActiveEye Remote Security Sensor (AERSS)	Number of sensors:		Yes/No
Log Collection / Analytics	Online Storage: 30 days Extended Log Storage: 12 Months		Yes/No
Network Detection	Up to 1 Gbps per sensor port		Yes/No
Endpoint Detection and Response	Cortex XDR		
External Vulnerability Scanning			Yes/No
Advanced Threat Insights	**Section 2** # of hours included		

The following table lists any ancillary components required.

Description	Quantity
Internetworking Firewall	
Control Room Firewall	

4.1.1.9 Limitations and Exclusions

This section applies to all cybersecurity services contained in the Statement of Work. Managed Detection and Response does NOT include services to perform physical containment and/or remediation of confirmed security incidents, remote or onsite. The Customer may choose to purchase additional Incident Response professional services to assist in the creation of and/or execution of a Customer's Incident Response Plan.

Motorola's scope of services does not include responsibilities relating to recovery of data available through the products or services, or remediation or responsibilities relating to the loss of data, ransomware, or hacking.

Motorola does not represent that it will identify, fully recognize, discover or resolve all security events or threats, system vulnerabilities, malicious codes, files or malware, indicators of compromise or internal threats or concerns

NOTWITHSTANDING ANY PROVISION OF THE AGREEMENT TO THE CONTRARY, MOTOROLA WILL HAVE NO LIABILITY FOR (A) INTERRUPTION OR FAILURE OF CONNECTIVITY, VULNERABILITIES, OR SECURITY EVENTS; (B) DISRUPTION OF OR DAMAGE TO CUSTOMER'S OR THIRD PARTIES' SYSTEMS, EQUIPMENT, OR DATA, INCLUDING DENIAL OF ACCESS TO USERS, OR SHUTDOWN OF SYSTEMS CAUSED BY INTRUSION DETECTION SOFTWARE OR HARDWARE; (C) AVAILABILITY OR ACCURACY OF ANY DATA AVAILABLE THROUGH THE SERVICES, OR INTERPRETATION, USE, OR MISUSE THEREOF; (D) TRACKING AND LOCATION-BASED SERVICES; OR (E) BETA SERVICES

Service Limitations

Cybersecurity services are inherently limited and will not guarantee that the Customer's system will be error-free or immune to security breaches as a result of any or all of the services described in this SOW. Motorola does not warrant or guarantee that this service will identify all cybersecurity incidents that occur in the Customer's system. Services and deliverables are limited by, among other things, the evolving and often malicious nature of cyber threats, conduct/attacks, as well as the complexity/disparity and evolving nature of Customer computer system environments, including supply chains, integrated software, services, and devices. To the extent we do offer recommendations in connection with the services, unless otherwise stated in the Statement of Work, our recommendations are necessarily subjective, may or may not be correct, and may be based on our assumptions relating to the relative risks, priorities, costs and benefits that we assume apply to you.

Processing of Customer Data in the United States and/or Other Locations.

Customer understands and agrees that data obtained, accessed, or utilized in the performance of the services may be transmitted to, accessed, monitored, and/or otherwise processed by Motorola in the U.S. and/or other Motorola operations globally. Customer consents to and authorizes all such processing and agrees to provide, obtain, or post any necessary approvals, consents, or notices that may be necessary to comply with applicable law.

Customer and Third-Party Information

Customer understands and agrees that Motorola may obtain, use and/or create and use, anonymized, aggregated and/or generalized Customer Data, such as data relating to actual and potential security threats and vulnerabilities, for its lawful business purposes, including improving its services and sharing and leveraging such information for the benefit of Customer, other customers, and other interested parties. For avoidance of doubt, so long as not specifically identifying the Customer, Customer Data shall not include, and Motorola shall be free to use, share and leverage security threat intelligence and mitigation data generally, including without limitation, third party threat vectors and IP addresses (i.e., so long as not defined as personal information under applicable law), file hash information, domain names, malware signatures and information, information obtained from third party sources, indicators of compromise, and tactics, techniques, and procedures used, learned or developed in the course of providing Services, which data shall be deemed Service Use Data (i.e., Motorola data).

Third-Party Software and Service Providers, Including Resale

Motorola may use, engage, license, resell, interface with or otherwise utilize the products or services of third-party processors or sub-processors and other third-party software, hardware, or services providers (such as, for example, third-party endpoint detection and response providers). Such processors and sub-processors may engage additional sub-processors to process personal data and other Customer Data. Customer understands and agrees that the use of such third-party products and services, including as it relates to any processing or sub-processing of data, is subject to each respective third-party's own terms, licenses, End User License Agreements (EULA), privacy statements, data processing agreements and/or other applicable terms. Such third-party providers and terms may

include the following, if applicable, or as otherwise made available publicly, through performance, or upon request:

Third Party Provider	Links
Palo Alto	EULA: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-end-user-license-agreement-eula.pdf Customer Data Processing Addendum: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo_alto_networks_customer_data_processing_agreement.pdf

Motorola disclaims any and all responsibility for any and all loss or costs of any kind associated with security events. Motorola disclaims any responsibility for customer use or implementation of any recommendations provided in connection with the services. Implementation of recommendations does not ensure or guarantee the security of the systems and operations evaluated.

4.1.2 Network Event Monitoring

Network Event Monitoring provides continuous real-time fault monitoring for radio communications networks. Motorola uses a defined set of tools to remotely monitor the Customer's ASTRO 25 radio network and characterize network events. When an actionable event takes place, it becomes an incident. CMSO technologists acknowledge and assess these incidents, and initiate a defined response.

4.1.2.1 Description of Service

With Network Event Monitoring, Motorola uses a Managed Services Suite of Tools (MSST) to detect events 24/7 as they occur, analyze them, and escalate them to the Network Operation Center (NOC). Incidents will be generated automatically based on the criteria shown in Table 4-3: Alarm Threshold Rule Options for all Event Types.

Table 4-3: Alarm Threshold Rule Options for all Event Types

Standard Threshold	Optional Threshold
An incident will be triggered if an event fulfills one of the two following criteria: ▪ Event occurs 5 times in 30 minutes. ▪ Event causes 10 minutes of continuous downtime for a monitored component.	An incident will be triggered if an event fulfills one of the two following criteria: ▪ Event occurs 7 times in 30 minutes. ▪ Event causes 15 minutes of continuous downtime for a monitored component.

The CMSO NOC agent assigns a priority level to an incident, then initiates a response in accordance with the Customer Handling Procedure (CHP). Depending on the incident, Motorola's response may include continued monitoring for further incident development, remote remediation by technical support, dispatching a field service technician, or other actions Motorola determines necessary.

To prevent duplicate incidents from being generated by the same root cause, Motorola employs an auto triage process that groups related incidents. The auto triage process therefore automatically assigns grouped incidents to a field service technician, enabling the resolution of these incidents together if the root alarm has been addressed.

Motorola uses a set of standard templates to record key information on service process, defined actions, and points of contact for the Customer's service. In the event of an incident, Motorola and the Customer can reference these templates. When information is updated, it will be organized in four categories:

- **Open** – Motorola's points of contact for dispatch permissions, entitlement information, and knowledge management.
- **Vendor** – Escalation and contact information.
- **Resolution** – Incident closure information.
- **Site Arrival** – Site arrival and exit process information.

The Customer will be able to access information on Network Event Monitoring activities via Customer Hub, including incident management reports. Any specific remediation and action notes from Motorola's CMSO or field service technicians will be available for the Customer to review as well.

Service Configuration Portal-Lite (SCP-Lite), which can be accessed through Customer Hub, provides a read-only view of the Customer's current service configuration, including site parameters, notification preferences and dispatch information. If the Customer or Motorola makes changes to the network, the updated information will be incorporated into SCP-Lite allowing the Customer a view of the ASTRO 25 radio network's state.

4.1.2.2 Scope

Network Event Monitoring is available 24/7. Incidents generated by the monitoring service will be handled in accordance with Section 5: Priority Level Definitions and Response Times.

Network Event Monitoring is a globally provided service unless limited by data export control or other applicable local and regional regulations. Timeframes are based on the Customer's local time zone.

4.1.2.3 Inclusions

Network Event Monitoring is available for the devices listed in Section 4.1.2.6: Monitored Elements.

Motorola Responsibilities

- Provide a dedicated network connection necessary for monitoring the Customer's communication network. **Section 4.1.2.4: Connectivity** describes available connectivity options.
- If determined necessary by Motorola Solutions, provide Motorola Solutions-owned equipment at the Customer's premises for monitoring network elements. The type of equipment and location of deployment is listed in **Section 4.1.2.5: Motorola Owned and Supplied Equipment**.
- Verify connectivity and event monitoring prior to system acceptance or start date.
- Monitor system continuously during hours designated in the Customer Support Plan (CSP), and in accordance with **Section 5: Priority Level Definitions and Response Times**.
- Remotely access the Customer's system to perform remote diagnosis as permitted by the Customer pursuant to **Section 4.1.2.3: Customer Responsibilities**.
- Create an incident, as necessary. Gather information to perform the following:
  - Characterize the issue
  - Determine a plan of action

  - Assign and track the incident to resolution
- Provide the Customer with system configuration info, site info, system notifications, and system notes via Customer Hub.
- Cooperate with the Customer to coordinate the transition of monitoring responsibilities between Motorola Solutions and the Customer as specified in **Section 4.1.2.3: Customer Responsibilities**.
- Maintain communication as needed with the Customer in the field until incident resolution.
- Provide available information on incident resolution to the Customer.

Limitations and Exclusions

The following activities are outside the scope of the Network Monitoring service:

- Motorola will not monitor any elements outside of the Customer's ASTRO 25 network, or monitor infrastructure provided by a third-party, unless specifically stated. Monitored elements must be within the ASTRO 25 radio network and capable of sending alerts to the Unified Event Manager (UEM).
- Additional support charges above contracted service agreement fees may apply if Motorola determines that system faults were caused by the Customer making changes to critical system parameters without written agreement from Motorola.
- Monitoring of network transport, such as WAN ports, WAN cloud, and redundant paths, unless provided by supplemental service outside this standard scope.
- Elements deployed outside of ASTRO RNI (E.g.: ASTRO CEN sites) are excluded from the service.
- Emergency on-site visits required to resolve technical issues that cannot be resolved by working remotely with the Customer's technical resource.
- System installations, upgrades, and expansions.
- Customer training.
- Hardware repair and/or replacement.
- Network security services.
- Information Assurance.

Customer Responsibilities

- Allow Motorola Solutions continuous remote access to enable the monitoring service.
- Provide continuous utility service to any Motorola Solutions equipment installed or used at the Customer's premises to support delivery of the service. The Customer agrees to take reasonable due care to secure the Motorola Solutions equipment from theft or damage while on the Customer's premises.
- Prior to contract start date, provide Motorola Solutions with pre-defined information necessary to complete a CSP, including:
  - Incident notification preferences and procedure.
  - Repair verification preference and procedure.
  - Database and escalation procedure forms.

- Submit timely changes in any information supplied to Motorola Solutions and included in the CSP to the Customer Support Manager (CSM).
- Notify the CMSO when the Customer performs any activity that impacts the system. Activity that impacts the system may include, but is not limited to: installing software or hardware upgrades, performing upgrades to the network, renaming elements or devices within the network, and taking down part of the system to perform maintenance.
- Send system configuration change requests to Motorola Solutions' CSM via Customer Hub.
- Allow Motorola Solutions' field service technician, if designated in the CSP, access to equipment, including any connectivity or monitoring equipment, if remote service is not possible.
- Allow Motorola Solutions' field service technician, if designated in the CSP, access to remove Motorola Solutions-owned monitoring equipment upon cancellation of service.
- Provide Motorola Solutions with all Customer-managed passwords required to access the Customer's system upon request, when opening a request for service support, or when needed to enable response to a technical issue.
- Pay additional support charges above the contracted service agreements that may apply if it is determined that system faults were caused by the Customer making changes to critical system parameters without written agreement from Motorola Solutions.
- In the event that Motorola Solutions agrees in writing to provide supplemental monitoring for third-party elements provided by the Customer, the Customer agrees to obtain third party consents or licenses required to enable Motorola Solutions to provide the monitoring service.
- Cooperate with Motorola Solutions and perform reasonable or necessary acts to enable Motorola Solutions to provide these services.
- Contact Motorola Solutions to coordinate transition of monitoring when the responsibility for monitoring needs to be transferred to or from Motorola Solutions, as specified in pre-defined information provided in the Customer's CSP. An example of a transfer scenario is transferring monitoring from Motorola Solutions for network monitoring after normal business hours.
  - Upon contact, the Customer must provide Motorola Solutions with customer name, site ID, status on any open incidents, priority level of any open incidents, brief descriptions of any ongoing incident, and action plan for resolving those incidents.
- Acknowledge that incidents will be handled in accordance with **Section 5: Priority Level Definitions and Response Times**.

4.1.2.4 Connectivity

The connectivity between customer's system and Motorola CMSO to enable Network Event Monitoring, MDR and RSUS should be established prior service start date.

Table 4-4: Available Connectivity

System Type	Available Connectivity	Set up and Maintenance
ASTRO 25	ASTRO Connectivity Service	Motorola

4.1.2.5 Motorola Owned and Supplied Equipment

This table identifies equipment that Motorola will supply to support the network monitoring service for the duration of the service.

Table 4-5: Motorola Owned and Supplied Equipment

Equipment Type	Location Installed
Firewall/Router	Primary Site
Service Delivery Management Server (DSR only)	Primary Site for each Zone

4.1.2.6 Monitored Elements

This table identifies the elements that can be monitored by the service. The specific quantities of each element to be monitored on the Customer's system will be inventoried in the CHP.

Table 4-6: Monitored Elements

Monitored Elements		
Active Directory	Enrichment Testing	Probe
Agent	Environmental	Core Switch
AIS	ESX	Radio Interface
AMB	Exit Router	RDM
Application Server	RNI Firewall	RFDS
APX Cloud Application	Core Server	RGU
ATR	Gateway	RNG
AUC	Gateway Router	Site Router
Backup Server	Gateway Unit	RTU
Base Radio	GIS Server	SCOM Server
Call Processor	HSS	Short Data Router
Camera	Install Server	Statistical Server
CBSD	Site Switch	Storage Networking
CCGW	Licensing Service	Consoles
Channel	Load Balancer	TRAK
Client Station	Logging Recorder	Terminal Server
CommandCentral AXS dispatch console	Logging Replay Station	Time Keeper
Controller	UNC	Training App
Conventional	UEM	Training Database
Core Router	MOSCAD Server	Trap Forwarder
Data Processing	Network Address	UCS
Database Server	Network Device	Licensing Server
Data Warehouse Server	NTP	Virtual Machine
Device Configuration Server	AIS	VMS

Monitored Elements		
DNS	Application Server	VPM
Domain Controller	Packet Data Gateway	WSGU
D series Site Controller	Physical Host Environmental	ZDS
eNodeB	Physical Host Power and Network	Zone Controller
Active directory	Power Distribution Unit	Syslog
Repeaters	Power Monitor	Proxy

4.1.3 ASTRO Connectivity Services

To establish a connection between the Customer's on-premises ASTRO 25 infrastructure core and Motorola Solutions Network and Security Operation Centers, Motorola will provide required network equipment with sufficient bandwidth as mentioned in Section 4.1.2.5: Motorola Owned and Supplied Equipment. The connectivity to customer's ASTRO 25 infrastructure core will terminate upon the Customer canceling their ASTRO 25 service package.

Motorola Responsibilities

Motorola will fulfill the following responsibilities to provide the ASTRO 25 Connectivity Service.

- Perform a site survey prior to installation to assess that all the conditions for a proper site installation can be met, including, but not limited to the presence of network facilities necessary to provide the necessary connectivity.
- Motorola will note any variations of the site that would affect the hardware specifications or estimated labor involved for a standard installation. If the site survey indicates a non-standard installation (for example, the need for construction of "last mile" network facilities), then a mutually agreed change order may be required.
- It is assumed that in the building, LTE coverage is adequate at the installation site. If, during installation, it is determined the in-building LTE coverage is not adequate for service, then a mutually agreed change order may be required for external antenna installation.
- Standard Demarc – Motorola will install cable between the Local Exchange Carrier Minimum Point of Entry (MPOE) and the Managed Elements located within the customer ASTRO infrastructure. Motorola will install the demarc standard – which includes one service call, up to two (2) total hours of on-site labor, and installation of one (1) cat 3, 5, or 5e cable drop up to 150 feet (vertical length up to 12 feet), connectors, ty-wraps, jacks, face plates, and cable. A mutually agreed change order may be required if the site survey indicates a non-standard extended demarc (for example, the need for cable through walls over 150' or multiple floors).
- Install equipment supplied by Motorola. Installation period is estimated to be within 45 business days from when Motorola and Customer execute the Agreement and related addendum or addenda.
- Cooperate with the Customer to schedule the ASTRO 25 Connectivity Service implementation.
- Administer safe work procedures for installation of the remote access circuit.

Customer Responsibilities

- Sign the Transport Connectivity Addendum (TCA).

- Provide space for the networking equipment at the core site.
- Ensure communications sites meet space, grounding, power, and connectivity requirements for equipment installation.
- Obtain all licensing, site access, or permitting required for project implementation.
- Provide a dedicated delivery point (such as a warehouse), for receipt, inventory, and storage of equipment prior to delivery to the site(s), if requested by Motorola.
- Ensure existing sites or equipment locations have sufficient space available for the system, as specified by Motorola's R56 Standards and Guidelines for Communication.
- Ensure that existing sites or equipment locations have adequate electrical power in the proper phase, in the proper voltage, and with necessary site grounding to support the requirements of the equipment provided with the ASTRO 25 Connectivity Service.
- Perform any location upgrades or modifications.
- Obtain and maintain approved local, State, or Federal permits necessary for installing and operating the proposed equipment.
- Provide any required system interconnections not specifically included in the ASTRO 25 Connectivity Service.
- Install demarcation equipment, air conditioning, and other equipment that is not provided by Motorola and is necessary to support the project.
- Perform work necessary to complete the connectivity provisioning outside the scope of the installation provided by Motorola.
- If Motorola’s design requires wireless backup and out-of-band (OOB) monitoring, Motorola may provide a wireless modem at the Customer location for OOB monitoring for Motorola Solutions Monitored Elements. The Customer shall provide access and accommodations to install the modem if required.
- The Customer will notify Motorola of any maintenance that may affect the operating status of the service using a Customer Maintenance Change Management Request via the Customer Hub. Examples of maintenance activities include: powering down the site, a Motorola Managed Element, or a third-party Network Terminating Unit; or, resetting, recabling, or moving equipment components.
- If a Motorola representative visits the Customer Site or works remotely, at the Customer’s request, to investigate an issue with the Service, and the Motorola representative determines the Service is functioning correctly or is prevented from resolving the issue because the Customer did not provide access or reasonable assistance, the Customer will be charged at published or negotiated time and material rates.
- Upon termination of the services, Customer shall promptly return to Motorola all equipment provided by Motorola in conjunction with the ASTRO 25 Connectivity Service and not explicitly owned by Customer. Motorola is entitled to invoice any and all costs arising out of or in connection with Customer’s failure to return the Motorola equipment if the Motorola equipment is not returned within sixty (60) days following termination of services.

Limitations/Exclusions

- Additional connectivity outside the scope of these services is not covered in this SOW.
- Motorola is not responsible for system faults or deficiencies that are caused by changes or modifications to the system not performed by Motorola.

4.1.4 Remote Technical Support

Motorola's Remote Technical Support service provides telephone consultation for technical issues that require a high level of ASTRO 25 network knowledge and troubleshooting capabilities. Remote Technical Support is delivered through the Motorola CMSO organization by a staff of technical support specialists skilled in diagnosis and swift resolution of infrastructure performance and operational issues.

Motorola applies leading industry standards in recording, monitoring, escalating, and reporting for technical support calls from its contracted customers to provide the support needed to maintain mission-critical systems.

4.1.4.1 Description of Service

The CMSO organization's primary goal is Customer Issue Resolution (CIR), providing incident restoration and service request fulfillment for Motorola's currently supported infrastructure. This team of highly skilled, knowledgeable, and experienced specialists is an integral part of the support and technical issue resolution process. The CMSO supports the Customer remotely using a variety of tools, including fault diagnostics tools, simulation networks, and fault database search engines.

Calls requiring incidents or service requests will be logged in Motorola's CRM system, and Motorola will track the progress of each incident from initial capture to resolution. This helps ensure that technical issues are prioritized, updated, tracked, and escalated as necessary, until resolution. Motorola will advise and inform Customer of incident resolution progress and tasks that require further investigation and assistance from the Customer's technical resources.

The CMSO Operations Center classifies and responds to each technical support request in accordance with Section 5: Priority Level Definitions and Response Times.

This service requires the Customer to provide a suitably trained technical resource that delivers maintenance and support to the Customer's system, and who is familiar with the operation of that system. Motorola provides technical consultants to support the local resource in the timely closure of infrastructure, performance, and operational issues.

4.1.4.2 Scope

The CMSO Service Desk is available via telephone 24/7 to receive and log requests for technical support. Remote Technical Support service is provided in accordance with Section 5: Priority Level Definitions and Response Times.

4.1.4.3 Inclusions

Remote Technical Support service will be delivered for Motorola-provided infrastructure, including integrated third-party products.

Motorola Responsibilities

- Maintain availability of the Motorola CMSO Service Desk via telephone (800-MSI-HELP) 24/7 to receive, log, and classify Customer requests for support.
- Respond to incidents and technical service requests in accordance with Section 5: Priority Level Definitions and Response Times.

- Provide caller a plan of action outlining additional requirements, activities, or information required to achieve restoral/fulfillment.
- Maintain communication with the Customer in the field as needed until resolution of the incident.
- Coordinate technical resolutions with agreed upon third-party vendors, as needed.
- Escalate support issues to additional Motorola technical resources, as applicable.
- Determine, in its sole discretion, when an incident requires more than the Remote Technical Support services described in this SOW and notify the Customer of an alternative course of action.

Limitations and Exclusions

The following activities are outside the scope of the Remote Technical Support service:

- Customer training.
- Remote Technical Support for network transport equipment or third-party products not sold by Motorola.
- Any maintenance and/or remediation required as a result of a virus or unwanted cyber intrusion.

Customer Responsibilities

- Prior to contract start date, provide Motorola with pre-defined information necessary to complete CSP.
- Submit timely changes in any information supplied in the CSP to the CSM.
- Contact the CMSO Service Desk to engage the Remote Technical Support service when needed, providing the necessary information for proper entitlement services. This information includes, but is not limited to, the name of contact, name of Customer, system ID number, site(s) in question, and a brief description of the problem that contains pertinent information for initial issue classification.
- Maintain suitably trained technical resources familiar with the operation of the Customer's system to provide field maintenance and technical maintenance services for the system.
- Supply suitably skilled and trained on-site presence when requested.
- Validate issue resolution in a timely manner prior to close of the incident.
- Acknowledge that incidents will be addressed in accordance with Section 5: Priority Level Definitions and Response Times.
- Cooperate with Motorola, and perform all acts that are reasonable or necessary to enable Motorola to provide Remote Technical Support.
- In the event that Motorola agrees in writing to provide supplemental Remote Technical Support to third-party elements provided by the Customer, the Customer agrees to obtain all third-party consents or licenses required to enable Motorola to provide the service.

4.1.5 Network Hardware Repair with Advanced Replacement (Not Included)

Motorola will provide hardware repair for Motorola and select third-party infrastructure equipment supplied by Motorola. A Motorola authorized repair depot manages and performs the repair of Motorola supplied equipment, and coordinates equipment repair logistics.

4.1.5.1 Description of Service

Infrastructure components are repaired at Motorola-authorized Infrastructure Depot Operations (IDO). At Motorola's discretion, select third-party infrastructure may be sent to the original equipment manufacturer or third-party vendor for repair.

Network Hardware Repair is also known as Infrastructure Repair.

4.1.5.2 Scope

Repair authorizations are obtained by contacting the CMSO organization Service Desk, which is available 24/7. Repair authorizations can also be obtained by contacting the CSM.

4.1.5.3 Inclusions

This service is available on Motorola-provided infrastructure components, including integrated third-party products. Motorola will make a commercially reasonable effort to repair Motorola manufactured infrastructure products after product cancellation. The post-cancellation support period of the product will be noted in the product's end-of-life (EOL) notification.

Motorola Responsibilities

- Provide the Customer access to the CMSO Service Desk, operational 24/7, to request repair service.
- Provide repair return authorization numbers when requested by the Customer.
- Receive malfunctioning infrastructure components from the Customer and document its arrival, repair, and return.
- Conduct the following services for Motorola infrastructure:
  - Perform an operational check on infrastructure components to determine the nature of the problem.
  - Replace malfunctioning components.
  - Verify that Motorola infrastructure components are returned to applicable Motorola factory specifications.
  - Perform a box unit test on serviced infrastructure components.
  - Perform a system test on select infrastructure components.
- Conduct the following services for select third-party infrastructure:
  - When applicable, perform pre-diagnostic and repair services to confirm infrastructure component malfunctions and prevent sending infrastructure components with No Trouble Found (NTF) to third-party vendor for repair.
  - When applicable, ship malfunctioning infrastructure components to the original equipment manufacturer or third-party vendor for repair service.
  - Track infrastructure components sent to the original equipment manufacturer or third-party vendor for service.
  - When applicable, perform a post-test after repair by original equipment manufacturer or third-party vendor to confirm malfunctioning infrastructure components have been repaired and function properly in a Motorola system configuration.

- Reprogram repaired infrastructure components to original operating parameters based on software and firmware provided by the Customer, as required in Section 4.1.5.3: Customer Responsibilities. If the Customer's software version and configuration are not provided, shipping will be delayed. If the repair depot determines that infrastructure components are malfunctioning due to a software defect, the repair depot reserves the right to reload these components with a different but equivalent software version.
- Properly package repaired infrastructure components.
- Ship repaired infrastructure components to Customer-specified address during normal operating hours of Monday through Friday from 7:00 a.m. to 7:00 p.m. Central Standard Time (CST), excluding holidays. Infrastructure component will be sent using two-day air shipping unless the Customer requests otherwise. Motorola will pay for shipping unless the Customer requests shipments outside of the above mentioned standard business hours or carrier programs, such as next flight out (NFO). In such cases, the Customer will be responsible for paying shipping and handling charges.

Limitations and Exclusions

Motorola may return infrastructure equipment that is no longer supported by Motorola, the original equipment manufacturer, or a third-party vendor without repairing or replacing it. The following items are excluded from this service:

- All Motorola radio infrastructure components over the post-cancellation support period.
- All third-party radio infrastructure components over the post-cancellation support period.
- All broadband infrastructure components over the post-cancellation support period.
- Physically damaged infrastructure components.
- Third-party equipment not shipped by Motorola.
- Consumable items including, but not limited to, batteries, connectors, cables, toner or ink cartridges, tower lighting, laptop computers, monitors, keyboards, and mouse.
- Video retrieval from digital in-car video equipment.
- RF infrastructure and backhaul components, including but not limited to, antennas, transmission lines, antenna dehydrators, microwave, line boosters, amplifiers (such as tower top amplifiers and bi-directional amplifiers), logging recorders, data talker wireless transmitters, short haul modems, combiners, multicouplers, duplexers, shelters, shelter HVAC, generators, UPS's, dropship nonstandard items and test equipment.
- Racks, furniture, and cabinets.
- Non-standard configurations, customer-modified infrastructure, and certain third-party dropship products.
- Firmware or software upgrades.

Customer Responsibilities

- Contact or instruct servicer to contact the Motorola CMSO organization, and request a return authorization number prior to shipping malfunctioning infrastructure components.
- Provide model description, model number, serial number, type of system, software and firmware version, symptom of problem, and address of site location for spare infrastructure components.
- Indicate if Motorola or third-party infrastructure components being sent in for service were subjected to physical damage or lightning damage.

- Follow Motorola instructions regarding including or removing firmware and software applications on infrastructure components being sent in for service.
- In the event that the Customer requires repair of equipment that is not contracted under this service at the time of request, the Customer acknowledges that charges may apply to cover shipping, labor, and parts. Motorola and the Customer will collaborate to agree on payment vehicle that most efficiently facilitates the work, commensurate with the level of urgency that is needed to complete the repair.
- Properly package and ship the malfunctioning component, at the Customer's expense. The Customer is responsible for properly packaging the malfunctioning infrastructure component to ensure it is not damaged in-transit and arrives in repairable condition.
  - Clearly print the return authorization number on the outside of the packaging.
- Maintain versions and configurations for software, applications, and firmware to be installed on repaired equipment.
- Provide Motorola with proper software and firmware information to reprogram equipment after repair, unless current software has caused this malfunction.
- Cooperate with Motorola and perform reasonable or necessary acts to enable Motorola to provide hardware repair services to the Customer.
- At the Customer's cost, obtain all third-party consents or licenses required to enable Motorola to provide the service.

4.1.5.4 Repair Process

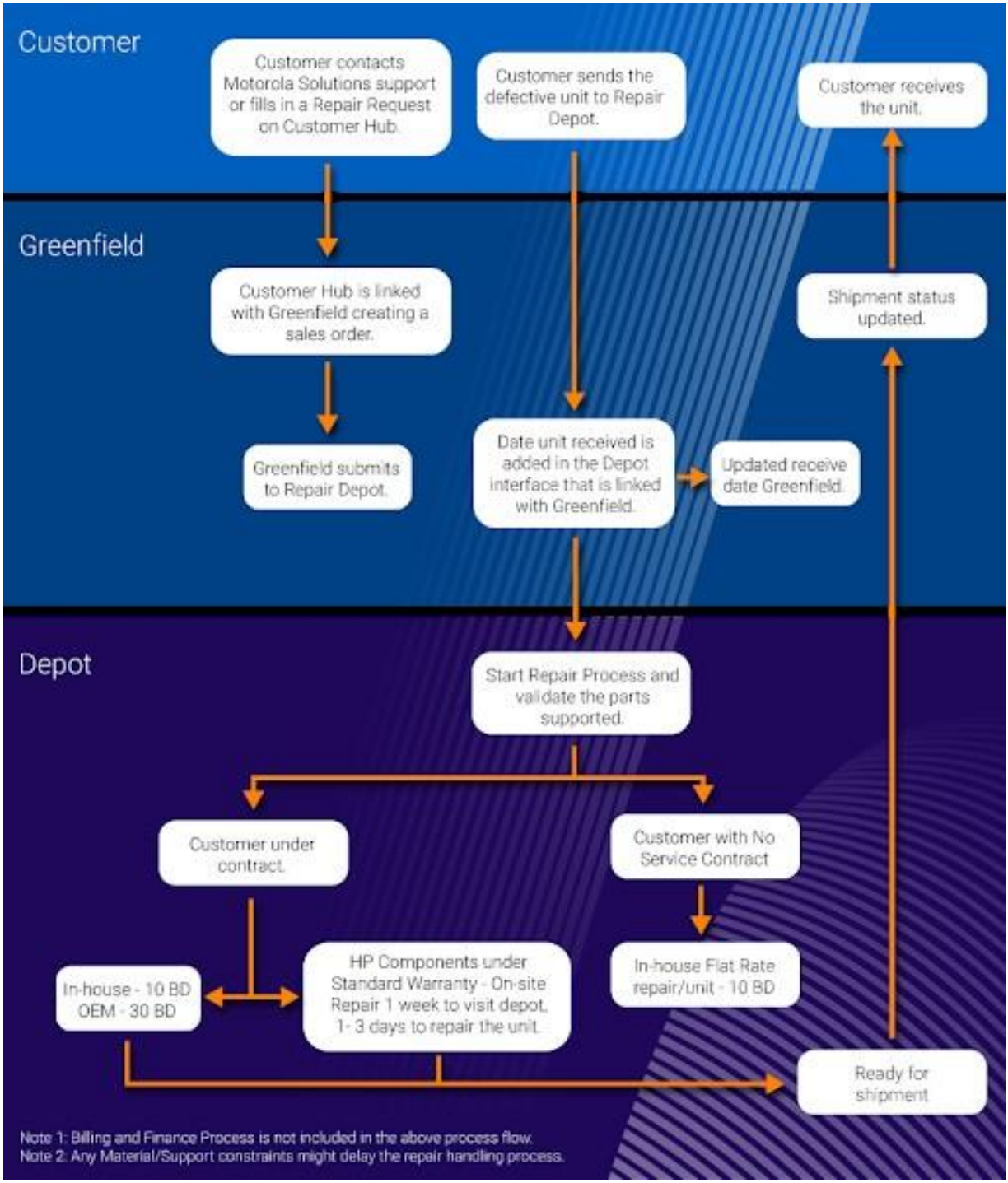

Figure 1: Repair Decision Process

4.1.5.5 Advanced Replacement-(Not Included)

As an addition to Hardware Repair service, Advanced Replacement is a repair exchange service for Motorola and select third-party infrastructure components supplied by Motorola. When available, Motorola will provide the Customer with advanced replacement units or Field Replacement Units (FRU) in exchange for the Customer's malfunctioning equipment within the Radio Network Infrastructure (RNI). A Motorola-authorized repair depot will evaluate and repair malfunctioning equipment, and add that equipment to the depot's FRU inventory after completing repairs.

Customers who prefer to maintain their own FRU inventory may request an FRU while their unit is being repaired. Refer to Figure 2: Advanced Replacement Decision Process for details on the unit loan process.

Added Motorola Responsibilities for Advanced Replacement

- Use commercially reasonable efforts to maintain FRU inventory on supported platforms.
- Provide new or reconditioned Radio Network Infrastructure (RNI), subject to availability. The FRU will be an equipment type and version similar to the Customer's malfunctioning component, and will contain equivalent boards and chips.
- Load firmware and software for equipment that requires programming. The Customer's software version information must be provided for the replacement FRU to be programmed accordingly. If the Customer's software version and configuration are not provided, shipping will be delayed.
- Package and ship FRU from the FRU inventory to Customer-specified address.
  - Motorola will ship FRU as soon as possible, depending on stock availability and requested configuration. FRU will be shipped during normal operating hours of Monday through Friday from 7:00 a.m. to 7:00 p.m. CST, excluding holidays. Motorola will pay for the shipping to the Customer, unless the Customer requests shipments outside of standard business hours or carrier programs, such as weekend or NFO shipment. In such cases, the Customer will be responsible for paying shipping and handling charges.
  - When sending FRU to the Customer, provide a return air bill in order for the Customer to send the Customer's malfunctioning component. The Customer's malfunctioning component will become property of the Motorola repair depot or select third-party replacing it, and the Customer will own the FRU.
- Provide repair return authorization (RA) number upon Customer request to replace infrastructure components that are not classified as an advanced replacement FRU.
- Provide a repair RA number so that returned components can be repaired and returned to FRU stock.
- Receive malfunctioning components from the Customer, carry out repairs and testing, and return it to the FRU stock.

Added Customer Responsibilities for Advanced Replacement

- Pay for Advanced Replacement FRU shipping from Motorola repair depot if the Customer requested shipping outside of standard business hours or carrier programs set forth in Section 4.1.5.5: Added Motorola Responsibilities for Advanced Replacement. See Table 4-7: Shipping Charges and Default Mail Service for shipping charge details.

- Properly package and ship the malfunctioning component using the pre-paid air-bill that arrived with the FRU. The Customer is responsible for properly packaging the malfunctioning infrastructure component to ensure that it is not damaged in transit and arrives in repairable condition. The Customer will be subject to a replacement fee for malfunctioning components returned improperly.
- Within five business days of receipt of the advanced replacement FRU from Motorola's FRU inventory, properly package the Customer's malfunctioning FRU and ship the malfunctioning Infrastructure to Motorola's repair depot for evaluation and repair. The Customer must send the return air bill back to the repair depot in order to facilitate proper tracking of the returned infrastructure. The Customer will be subject to a full replacement fee for FRU's not returned within five business days.
- At the Customer's expense and risk of loss, the Customer may send a malfunctioning Motorola or third-party infrastructure component for repairs before a replacement has been sent. In such cases, the malfunctioning component should be properly packaged and shipped to Motorola.
- Clearly print the return authorization number on the outside of the packaging.

4.1.5.5.1 Replacement Process for Advanced Replacement

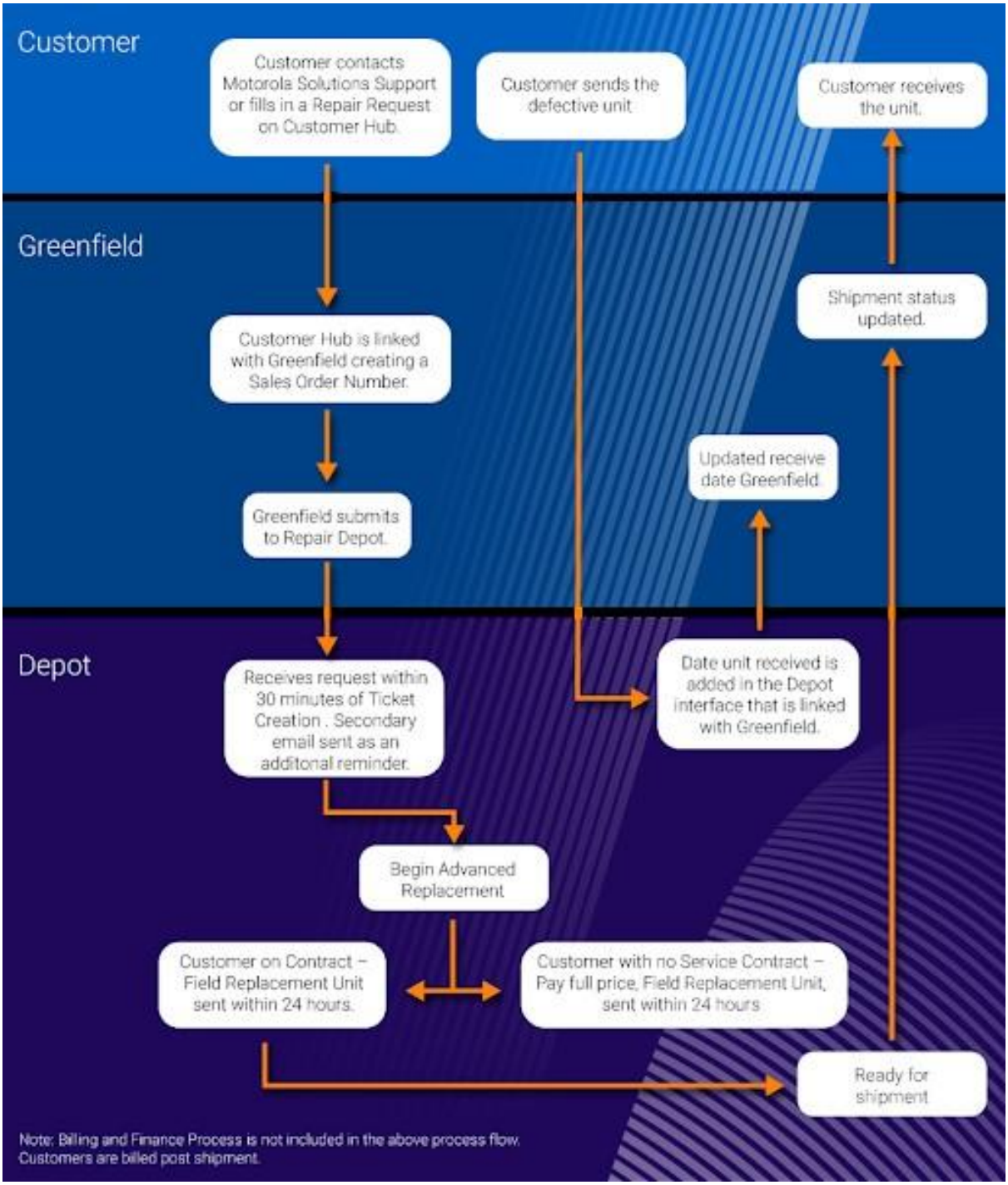

Figure 2: Advanced Replacement Decision Process

Table 4-7: Shipping Charges and Default Mail Service

Services	Advanced Replacement Charges Responsibility

Services	Advanced Replacement Charges Responsibility
Advanced Replacements (Normal Business Hours) Shipped FedEx Overnight or equivalent	Motorola
Shipping Outbound to Customer	
Repair and Return Shipping Outbound to Customer	
Advanced Replacements (Next Flight Out or Other)	Customer
Exchanges Shipped Outbound to Customer by Non-Motorola Carrier*	
Repair Shipping Inbound to Motorola	
Installation Labor	

Motorola shipping carrier – FedEx.

4.1.6 Security Update Service

Motorola's ASTRO 25 Security Update Service (SUS) provides pretested security updates, minimizing cyber risk and software conflicts. These security updates contain operating system security patches and antivirus definitions that have been validated for compatibility with ASTRO 25 systems. Security update delivery is determined by the options included as part of this service. Section 4.1.6.4: Inclusions indicates if options are included as part of this service.

4.1.6.1 Description of Service

Motorola uses a dedicated information assurance lab to test and validate security updates. Motorola deploys and tests security updates in the lab to check for and prevent potential service degradation.

Motorola releases tested, compatible security updates for download and installation. Once security updates are verified by the SUS team, Motorola uploads them to a secure website and sends a release notification email to the Customer contact to inform them that the security update release is available. If there are any recommended configuration changes, warnings, or workarounds, the SUS team will provide documentation with the security updates on the secure website.

Note, the ASTRO 25 Advanced Service also includes the Remote Security Update Service. See Section 4.1.7. Customer download and self-installation of security updates is only necessary for the system components that are not covered by RSUS. See **Appendix 1** for RSUS scope and exclusions.

For RSUS exclusions, with the base SUS service, the Customer will be responsible for downloading security updates, installing them on applicable components, and rebooting updated components.

Additional options are available for Motorola to deploy security updates, reboot servers and workstations, or both.

4.1.6.2 On-Site Delivery

If On-Site Delivery is included with SUS, Motorola provides trained technician(s) to install security updates at the Customer's location. The technician downloads and installs available security updates and coordinates any subsequent server and workstation reboots.

4.1.6.2.1 Reboot Support

If Reboot Support is included with RSUS, Motorola provides technician support to reboot impacted Microsoft Windows servers and workstations after operating system security patches have been installed.

4.1.6.3 Scope

RSUS includes pretested security updates for the software listed in Table 4-8: Update Cadence. This table also describes the release cadence for security updates.

Table 4-8: Update Cadence

Software	Update Release Cadence
Antivirus Definition Files	Weekly
Microsoft Windows	Monthly
Microsoft SQL Server	Quarterly
Microsoft Windows third party (i.e. Adobe Reader)	Monthly
Red Hat Linux (RHEL)	Quarterly
VMWare ESXi Hypervisor	Quarterly
PostgreSQL	Quarterly
McAfee Patch(es)	Quarterly
Dot Hill DAS Firmware	Quarterly
HP SPP Firmware	Quarterly
QNAP Firmware	Quarterly

4.1.6.4 Inclusions

Supported ASTRO 25 core types and security update delivery methods are included in Table 4-9: SUS Packages. This table indicates if Motorola will provide any SUS optional services to the Customer. SUS supports the current Motorola ASTRO 25 system release and aligns with the established Software Support Policy (SwSP).

Motorola reserves the right to determine which releases are supported as business conditions dictate. Additional charges may apply in the event of supporting older releases. Contact Motorola's assigned CSM for the latest supported releases.

Table 4-9: SUS Packages

Service	ASTRO 25 Core Type	Included
Security Update Service Customer Self-installed	L Core M Core Simplified Core	X

Service	ASTRO 25 Core Type	Included
Security Update Service with Reboot Support	L Core M Core Simplified Core	
Security Update Service with On-Site Delivery	L Core M Core Simplified Core	

Responsibilities for downloading and installing security updates and rebooting applicable hardware are detailed in Section 4.1.6.5: Installation and Reboot Responsibilities.

Motorola Responsibilities

- On the release schedule in Section 4.1.6.3: Scope review relevant and appropriate security patches released by Original Equipment Manufacturer (OEM) vendors.
- Release tested and verified security patches to Motorola's secure website.
- Publish documentation for installation, recommended configuration changes, any identified issue(s), and remediation instructions for each security update release.
- Send notifications by email when security updates are available to download from the secure website.

Limitations and Exclusions

- Systems with non-standard configurations that have not been certified by Motorola's Systems Integration and Test (SIT) team are specifically excluded from this service, unless otherwise agreed in writing by Motorola.
- Interim or unplanned releases outside the supported release cadence.
- Service does not include pretested intrusion detection system (IDS) signature updates for IDS solutions.
- This service does not include releases for Motorola products that are not ASTRO 25 L, M, and Simplified Core radio network infrastructure equipment. The following are examples of excluded products: WAVE PTX™, Critical Connect, and VESTA® solutions.
- K Core ASTRO 25 systems are excluded.
- Motorola product updates are not included in these services.
- Shared network infrastructure firmware, such as transport and firewall firmware are not included in these services.
- Motorola does not represent that it will identify, fully recognize, discover, or resolve all security events or threats, system vulnerabilities, malicious codes or data, backdoors, or other system threats or incompatibilities as part of the service, or that the agreed upon cadence/time of delivery will be sufficient to identify, mitigate or prevent any cyber incident.

Customer Responsibilities

- Provide Motorola with predefined information necessary to complete a Customer Support Plan (CSP) prior to the Agreement start date.

- Provide timely updates on changes of information supplied in the CSP to Motorola's assigned CSM.
- Update Motorola with any changes in contact information, specifically for authorized users of Motorola's secure website.
- Provide means for accessing Motorola's secure website to collect the pretested files.
- Download and apply only to the Customer's system as applicable, based on the Customer Agreement and the scope of the purchased service. Distribution to any other system or user other than the system/user contemplated by the Customer Agreement is not permitted.
- Implement Motorola Technical Notices (MTN) to keep the system current and patchable.
- Adhere closely to the Motorola Solutions Centralized Managed Support Operations (CMSO) troubleshooting guidelines provided upon system acquisition. Failure to follow CMSO guidelines may cause the Customer and Motorola unnecessary or overly burdensome remediation efforts. In such cases, Motorola reserves the right to charge an additional fee for the remediation effort.
- Upgrade system to a supported system release when needed to continue service. Contact Motorola's assigned CSM for the latest supported releases.
- Comply with the terms of applicable license agreements between the Customer and non-Motorola software copyright owners.

4.1.6.5 Installation and Reboot Responsibilities

Installation and Reboot responsibilities are determined by the specific SUS package being purchased. Table 4-10: Installation and Reboot Responsibilities Matrix contains the breakdown of responsibilities. Section 4.1.6.4: Inclusions indicates which services are included.

Microsoft Windows servers and workstations often need to be rebooted before security updates take full effect and mitigate vulnerabilities.

Table 4-10: Installation and Reboot Responsibilities Matrix

SUS Package	Motorola Responsibilities	Customer Responsibilities
Security Update Service Customer Self-installed		▪ Deploy pretested files to the Customer's system as instructed in the "Read Me" text provided on Motorola's secure website. ▪ When a security update requires a reboot, reboot servers and workstations after security updates are installed.
Security Update Service with On-Site Delivery	▪ Dispatch a technician to deploy pretested files to the Customer's system. ▪ When a security update requires a reboot, reboot servers and workstations after security updates are installed.	▪ Acknowledge Motorola will reboot servers and workstations, and agree to timing.

SUS Package	Motorola Responsibilities	Customer Responsibilities
Security Update Service with Reboot Support	▪ When a security update requires a reboot, dispatch a technician to reboot servers and workstations after security updates are installed.	▪ Deploy pretested files to the Customer's system as instructed in the "Read Me" text provided on Motorola's secure website.

Disclaimer

This service tests OEM security updates. Delivering security updates for specific software depends on OEM support for that software. If an OEM removes support (e.g. end-of-life) from deployed software, Motorola may work with the OEM to reduce the impact, but may remove support for the affected software from this service without notice.

OEMs determine security update schedules, supportability, or release availability without consultation from Motorola. Motorola will obtain and test security updates when they are made available, and incorporate those security updates into the next appropriate release.

All security updates are important. This service is intended to balance the security and compatibility of tested updates with agreed upon time/cadence of delivery. Customer assumes the risk of this inherent tradeoff.

Motorola disclaims any warranty with respect to pretested database security updates, hypervisor patches, operating system software patches, intrusion detection sensor signature files, or other third-party files, express or implied. Further, Motorola disclaims any warranty concerning non-Motorola software and does not guarantee Customers' systems will be error-free or immune to security breaches as a result of these services.

4.1.7 Remote Security Update Service

Motorola's ASTRO 25 Remote Security Update Service (RSUS) provides pretested security updates, minimizing cyber risk and software conflicts. These security updates contain operating system security patches and antivirus definitions that have been validated for compatibility with ASTRO 25 systems. Motorola will remotely deliver tested security updates to the Customer using a network connection. Reboot responsibility is determined by which options are included as part of this service.

The ASTRO 25 Monthly Security Update Service (SUS) is a prerequisite for RSUS. Please see the Statement of Works for: ASTRO 25 SUS Statement of Work.

4.1.7.1 Description of Service

Motorola remotely installs pretested security updates on the applicable ASTRO 25 system components, as defined in Appendix 1.

Note that some ASTRO 25 system components may be covered by the self-installed SUS service and not RSUS (RSUS Exceptions).

If the Customer is unable to apply updates to RSUS exceptions, Motorola can provide On-Site SUS, whereby the Motorola field service team attend Customer premises to install the updates.

Motorola remotely installs pretested security updates on the applicable ASTRO 25 system components. Motorola tests security updates for compatibility with ASTRO 25 in a dedicated information assurance lab.

Motorola will install compatible ASTRO 25 security updates using a remote connection. After installing tested security updates remotely, Motorola provides the Customer with a report outlining the updates made to the Customer's system. This report will inform the Customer of security update network transfers and installation statuses.

4.1.7.1.1 Application of Prerequisite Motorola Technical Notices (MTN)

In some instances, MTNs must be applied to enable Motorola to remotely deploy the latest security updates. MTN installation is not part of RSUS. In the event that Motorola is prevented from deploying security updates due to incomplete implementation of prerequisite MTNs, Motorola will raise a service incident and notify the Customer. Once necessary MTNs are applied to the Customer's system, Motorola will continue to remotely deploy security updates.

4.1.7.1.2 Updates to System Components in the Customer Enterprise Network

Connections to other networks, herein referred to as Customer Enterprise Network (CEN), are delineated by firewalls. All security updates deployed by RSUS are specific to the equipment included in the ASTRO 25 radio network. The only exceptions are those identified as RSUS exceptions in Appendix 1.

The Customer may request a quote, via the CSM, for Motorola to remotely install updates to eligible systems that are in the Customer's CEN.

The Customer must make the appropriate configuration changes to their firewall giving logical access and a network path to allow Motorola to remotely install the requisite patches.

4.1.7.1.3 Microsoft Windows Reboot Following Security Update Installation

It is a critical requirement for Microsoft Windows systems to be rebooted following the installation of security updates. In the case of RSUS, this is the responsibility of the Customer.

Failure of the Customer to fulfill reboot responsibilities as described in Table 4-13: Reboot Responsibilities Matrix exposes systems to security threats. Until reboot, the system is not updated.

It will also delay execution of future RSUS updates, with a risk of failed RSUS scheduling and unnecessary Customer impact.

If Customers require further support from Motorola to reboot following Microsoft Windows update deployment and installation, please contact your CSM who can discuss options for Reboot Support.

4.1.7.1.4 Reboot Support

If the Reboot Support service is sold to complement RSUS, Motorola provides technician(s) to reboot impacted Microsoft Windows servers and workstations after operating system security patches have been installed.

- The RSUS team will notify all listed contacts one week prior to patching to all required contacts (identified during service onboarding).

- On completion of patching, a final report is sent via email to the listed contacts.
- The notification will state that patching is complete and systems need to be rebooted.
- This process is repeated monthly.

Reboot Support requires that the Customer representative works with Motorola technicians to plan when reboots will be undertaken to reduce the operational impact.

4.1.7.2 Scope

RSUS includes pretested security updates for the software listed in Table 4-11: Update Cadence. This table also describes the release cadence for security updates.

Table 4-11: Update Cadence

Antivirus Definition Files	Weekly
Microsoft Windows	Monthly
Microsoft SQL Server	Quarterly
Red Hat Linux (RHEL)	Quarterly
VMWare ESXi Hypervisor	Quarterly
Trellix (McAfee) Patch(es)	Quarterly
Dot Hill DAS Firmware	Quarterly
HP SPP Firmware	Quarterly

Motorola installs security updates during normal business hours. Normal business hours are defined as 8 a.m. to 5 p.m. Central Standard Time Monday through Friday, excluding public holidays.

The Customer may submit a formal request that Motorola personnel work outside of these hours. The Customer will need to pay additional costs for work to be completed outside of normal business hours.

Motorola will provide an Impact Timeline (ITL) to the Customer to show installation tasks scheduled, including preparation work and the transfer of security updates to local storage or memory. Core Server reboots or zone controller rollover will be initiated at the times shared in the ITL.

It is a critical requirement that Microsoft Windows systems are rebooted following the installation of security updates. In the case of RSUS, this is the responsibility of the Customer.

Intrusive security updates require Customer coordination, may require hardware reboots and zone controller rolling (switching from one zone controller to the other) to fully implement. Systems with redundant zone controllers (M3) have low downtime (minutes) as the zone controllers are rolled but systems with single zone controllers will be down for longer periods. While rolling the zone controllers, the system will operate in “site trunking” mode. The Customer will need to be aware of these operational impacts, and coordinate events with users.

4.1.7.3 Tenanted Customers Access to Antivirus Updates

Where a Customer is a Tenant Customer (for example, a Public Safety Access Point / Dispatch Center) on a Core system owned and operated by another organization, any Tenant customer systems such as dispatch consoles need to be able to access the core Central Security Management Server (CSMS).

The RSUS team will need permission from the Core system owners to allow connectivity from the Core system to any RSUS entitled Tenant Customers.

4.1.7.4 Inclusions

Supported ASTRO 25 core types and security update delivery methods are included in Table 7: SUS Options. This table indicates if Motorola will provide any RSUS optional services to the Customer. RSUS supports the current Motorola ASTRO 25 system release and aligns with the established Software Support Policy (SwSP).

Motorola reserves the right to determine which releases are supported as business conditions dictate. Additional charges may apply in the event of supporting releases that are no longer within the Standard Support Period (as defined by the SWSP). Contact Motorola's assigned CSM for the latest supported releases.

Table 4-12: RSUS Options

Service	ASTRO 25 Core Type	Included
Remote Security Update Service	L Core M Core Simplified Core	Yes
Remote Security Update Service with Reboot Support	L Core M Core Simplified Core	(quoted)

Responsibilities for rebooting applicable hardware are detailed in Section 4.1.7.5: Reboot Responsibilities.

Motorola Responsibilities

- Remotely deploy patches listed in 4.1.8.2: Scope on the Customer's system. Patches will be installed on the cadence described in that section.
  - As outlined in 4.1.8.2: Scope, coordinate and communicate with the Customer when installing updates that will require server reboots, workstation reboots, or both.
  - Install non-intrusive updates, like antivirus definitions, as released without coordination.
- In the event that no security updates are released by the Original Equipment Manufacturers (OEM), the Final RSUS Patch Report can be reviewed by the Customer to identify where no new security updates were required.
- Coordinate RSUS activities with any other Motorola system maintenance or other engineering activities with the Customer to minimize downtime, inefficiency and operational impact.

Limitations and Exclusions

- Systems with non-standard configurations that have not been certified by Motorola's Systems Integration and Test (SIT) team are specifically excluded from this service, unless otherwise agreed in writing by Motorola.
- Interim or unplanned releases outside the supported release cadence.
- Service does not include pretested intrusion detection system (IDS) signature updates for IDS solutions.

- This service does not include releases for Motorola products that are not ASTRO 25 L, M, and Simplified Core radio network infrastructure equipment. The following are examples of excluded products: WAVE PTX, Critical Connect, and VESTA solutions.
- K Core ASTRO 25 systems are excluded.
- Motorola product updates are not included in these services.
- Shared network infrastructure firmware, such as transport and firewall firmware are not included in these services.
- This service excludes the delivery of MTNs to the customer system.
- Motorola does not represent that it will identify, fully recognize, discover, or resolve all security events or threats, system vulnerabilities, malicious codes or data, backdoors, or other system threats or incompatibilities as part of the service, or that the agreed upon cadence/time of delivery will be sufficient to identify, mitigate or prevent any cyber incident.
- Motorola shall provide Customers with a list of MTNs that are prerequisite for execution of the RSUS service.

Customer Responsibilities

- This service requires connectivity from Motorola to the Customer's ASTRO 25 system. If required, procure internet connectivity before the service commences, and maintain it for the duration of the service contract.
- Refrain from making uncertified changes to the ASTRO 25 system. Consult with Motorola before making changes to the ASTRO 25 system.
- Be aware of the operational impacts of RSUS update installation, and coordinate the update process with users.
- Prerequisite Motorola Technical Notices (MTN) must be applied to enable Motorola to remotely deploy the latest security updates. The list of MTNs that must be applied are available on the SUS secure customer portal.

4.1.7.5 Reboot Responsibilities

Microsoft Windows servers and workstations often need to be rebooted before security updates take full effect and mitigate vulnerabilities. Reboot responsibilities are determined by the specific RSUS package being purchased. Table 4-13: Reboot Responsibilities Matrix contains the breakdown of responsibilities. Section 4.1.8.4: Inclusions indicates which services are included.

If a Customer chooses not to reboot after an update, whether for operational reasons or convenience, they are accepting the associated risks, which include:

- Greater exposure to cyber security threats and vulnerabilities.
- Impact to implementation of subsequent RSUS Microsoft Windows updates at the agreed delivery cadence, until the devices are rebooted and at the correct RSUS release.

If Customers require further support from Motorola to reboot following Microsoft Windows update deployment and installation, please contact your CSM who can discuss options for Reboot Support.

Table 4-13: Reboot Responsibilities Matrix

Remote SUS Package	Motorola Responsibilities	Customer Responsibilities

Remote SUS Package	Motorola Responsibilities	Customer Responsibilities
Remote Security Update Service	▪ Provide a report to the Customer's main contact listing the servers or workstations which must be rebooted to ensure installed security updates become effective.	▪ When a security update requires a reboot, reboot servers and workstations after security updates are installed. ▪ When remote deployment is in progress, it may be necessary for multiple reboots to be coordinated with Motorola.
Remote Security Update Service with Reboot Support	▪ When a security update requires a reboot, dispatch a technician to reboot servers and workstations after security updates are installed.	▪

Disclaimer

This service tests OEM security updates. Delivering security updates for specific software depends on OEM support for that software. If an OEM removes support (e.g. end-of-life) from deployed software, Motorola may work with the OEM to reduce the impact, but may remove support for the affected software from this service without notice.

OEMs determine security update schedules, supportability, or release availability without consultation from Motorola. Motorola will obtain and test security updates when they are made available, and incorporate those security updates into the next appropriate release.

All security updates are important. This service is intended to balance the security and compatibility of tested updates with agreed upon time/cadence of delivery. Customer assumes the risk of this inherent tradeoff.

Motorola disclaims any warranty with respect to pretested database security updates, hypervisor patches, operating system software patches, intrusion detection sensor signature files, or other third-party files, express or implied. Further, Motorola disclaims any warranty concerning non-Motorola software and does not guarantee Customers' systems will be error-free or immune to security breaches as a result of these services.

4.1.8 On-Site Infrastructure Response

Motorola's On-Site Infrastructure Response service provides incident management and escalation for on-site technical service requests. The service is delivered by Motorola's CMSO organization in cooperation with a local service provider.

On-Site Infrastructure Response may also be referred to as On-Site Support.

4.1.8.1 Description of Service

The Motorola CMSO Service Desk will receive the Customer's request for on-site service.

The CMSO Dispatch Operations team is responsible for opening incidents, dispatching on-site resources, monitoring issue resolution, and escalating as needed to ensure strict compliance to committed response times.

The dispatched field service technician will travel to the Customer's location to restore the system in accordance with Section 4.1.8.5: Priority Level Definitions and Response Times.

Motorola will manage incidents as described in this SOW. The CMSO Service Desk will maintain contact with the field service technician until incident closure.

4.1.8.2 Scope

On-Site Infrastructure Response is available in accordance with Section 4.1.8.5: Priority Level Definitions and Response Times. Customer's Response Time Classification is designated in the Customer Support Plan.

4.1.8.3 Geographical Availability

On-Site Infrastructure Response is available worldwide where Motorola servicers are present. Response times are based on the Customer's local time zone and site location.

4.1.8.4 Inclusions

On-Site Infrastructure Response is provided for Motorola-provided infrastructure.

Motorola Responsibilities

- Receive service requests.
- Create an incident when service requests are received. Gather information to characterize the issue, determine a plan of action, and assign and track the incident to resolution.
- Dispatch a field service technician, as required by Motorola's standard procedures, and provide necessary incident information.
- Provide the required personnel access to relevant Customer information, as needed.
- Motorola field service technician will perform the following on-site:
  - Run diagnostics on the infrastructure component.
  - Replace defective infrastructure components, as supplied by the Customer.
  - Provide materials, tools, documentation, physical planning manuals, diagnostic and test equipment, and any other material required to perform the maintenance service.
  - If a third-party vendor is needed to restore the system, the vendor can be accompanied onto the Customer's premises.
  - If required by the Customer's repair verification in the CSP, verify with the Customer that restoration is complete or system is functional. If verification by the Customer cannot be completed within 20 minutes of restoration, the incident will be closed and the field service technician will be released.
  - Escalate the incident to the appropriate party upon expiration of a response time.
- Close the incident upon receiving notification from the Customer or Motorola field service technician, indicating the incident is resolved.
- Notify the Customer of incident status, as defined in the CSP and Service Configuration Portal (SCP):
  - Open and closed.
  - Open, assigned to the Motorola field service technician, arrival of the field service technician on-site, delayed, or closed.
- Provide incident activity reports to the Customer, if requested.

Limitations and Exclusions

The following items are excluded from this service:

- All Motorola infrastructure components beyond the post-cancellation support period.
- All third-party infrastructure components beyond the post-cancellation support period.
- All broadband infrastructure components beyond the post-cancellation support period.
- Physically damaged infrastructure components.
- Third-party equipment not shipped by Motorola.
- Consumable items including, but not limited to, batteries, connectors, cables, toner or ink cartridges, tower lighting, laptop computers, monitors, keyboards, and mouse.
- Video retrieval from digital in-car video equipment.
- RF infrastructure and backhaul components, including but not limited to, antennas, transmission lines, antenna dehydrators, microwave, line boosters, amplifiers (such as tower top amplifiers and bi-directional amplifiers), logging recorders, data talker wireless transmitters, short haul modems, combiners, multicouplers, duplexers, shelters, shelter HVAC, generators, UPS's, and test equipment.
- Racks, furniture, and cabinets.
- Tower and tower mounted equipment.
- Non-standard configurations, customer-modified infrastructure, and certain third-party infrastructure.
- Firmware or software upgrades.

Customer Responsibilities

- Contact Motorola, as necessary, to request service.
- Prior to start date, provide Motorola with the following pre-defined Customer information and preferences necessary to complete CSP:
  - Incident notification preferences and procedure.
  - Repair verification preference and procedure.
  - Database and escalation procedure forms.
- Submit timely changes in any information supplied in the CSP to the CSM.
- Provide the following information when initiating a service request:
  - Assigned system ID number.
  - Problem description and site location.
  - Other pertinent information requested by Motorola to open an incident.
- Provide field service technician with access to equipment.
- Supply infrastructure spare or FRU, as applicable, in order for Motorola to restore the system.
- Maintain and store software needed to restore the system in an easily accessible location.
- Maintain and store proper system backups in an easily accessible location.
- If required by repair verification preference provided by the Customer, verify with the CMSO Service Desk and dispatch that restoration is complete or system is functional.

- Cooperate with Motorola and perform reasonable or necessary acts to enable Motorola to provide these services.
- In the event that Motorola agrees in writing to provide supplemental On-Site Infrastructure Response to Customer-provided third-party elements, the Customer agrees to obtain and provide applicable third-party consents or licenses to enable Motorola to provide the service.

4.1.8.5 Priority Level Definitions and Response Times

This section describes the criteria Motorola used to prioritize incidents and service requests, and lists the response times for those priority levels.

Table 4-14: Standard Level Definitions and Response Times

Incident Priority	Incident Definition	On-Site Response Time
Critical P1	**Core**: Core server or core link failure. No redundant server or link available. **Sites/Subsites**: Primary site down. Two RF sites or more than 10% of RF sites down, whichever is greater. **Consoles**: More than 40% of a site's console positions down. **Conventional Channels**: Conventional Channel Gateways (CCGW) down without redundant gateways available. **Security Features**: Security is non-functional or degraded.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
High P2	**Core**: Core server or link failures. Redundant server or link available. **Consoles**: Between 20% and 40% of a site's console positions down. **Sites/Subsites**: One RF site or up to 10% of RF sites down, whichever is greater. **Conventional Channels**: Up to 50% of CCGWs down. Redundant gateways available. **Network Elements**: Site router, site switch, or GPS server down. No redundant networking element available.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
Medium P3	**Consoles**: Up to 20% of a site's console positions down. **Conventional Channels:** Single channel down. Redundant gateway available. **Network Elements**: Site router/switch or GPS server down. Redundant networking element available.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 8 hours of receiving dispatch notification.
Low P4	**Service Requests**: Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).	Not applicable.

Table 4-15: Premier Priority Level Definitions and Response Times

Incident Priority	Incident Definition	On-Site Response Time
Critical P1	**Core**: Core server or core link failure. No redundant server or link available. **Sites/Subsites**: Primary site down. Two RF sites or more than 10% of RF sites down, whichever is greater. **Consoles**: More than 40% of a site's console positions down. **Conventional Channels**: Conventional Channel Gateways (CCGW) down without redundant gateways available. **Security Features**: Security is non-functional or degraded.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 2 hours of receiving dispatch notification.
High P2	**Core**: Core server or link failures. Redundant server or link available. **Consoles**: Between 20% and 40% of a site's console positions down. **Sites/Subsites**: One RF site or up to 10% of RF sites down, whichever is greater. **Conventional Channels:** Up to 50% of CCGWs down. Redundant gateways available. **Network Elements**: Site router, site switch, or GPS server down. No redundant networking element available.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 2 hours of receiving dispatch notification.
Medium P3	**Consoles**: Up to 20% of a site's console positions down. **Conventional Channels**: Single channel down. Redundant gateway available. **Network Elements**: Site router/switch or GPS server down. Redundant networking element available.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 8 hours of receiving dispatch notification.
Low P4	**Service Requests**: Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).	Not applicable.

Table 4-16: Limited Priority Level Definitions and Response Times

Incident Priority	Incident Definition	On-Site Response Time

Incident Priority	Incident Definition	On-Site Response Time
Critical P1	**Core**: Core server or core link failure. No redundant server or link available. **Sites/Subsites**: Primary site down. Two RF sites or more than 10% of RF sites down, whichever is greater. **Consoles**: More than 40% of a site's console positions down. **Conventional Channels**: Conventional Channel Gateways (CCGW) down without redundant gateways available. **Security Features**: Security is non-functional or degraded.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
High P2	**Core**: Core server or link failures. Redundant server or link available. **Consoles**: Between 20% and 40% of a site's console positions down. **Sites/Subsites**: One RF site or up to 10% of RF sites down, whichever is greater. **Conventional Channels**: Up to 50% of CCGWs down. Redundant gateways available. **Network Elements**: Site router, site switch, or GPS server down. No redundant networking element available.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
Medium P3	**Consoles**: Up to 20% of a site's console positions down. **Conventional Channels**: Single channel down. Redundant gateway available. **Network Elements**: Site router/switch or GPS server down. Redundant networking element available.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 8 hours of receiving dispatch notification.
Low P4	**Service Requests**: Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).	Not applicable.

4.1.9 Annual Preventative Maintenance

Motorola personnel will perform a series of maintenance tasks to keep network equipment functioning correctly.

4.1.9.1 Description of Service

Annual Preventative Maintenance provides annual operational tests on the Customer's infrastructure equipment to monitor its conformance to specifications.

4.1.9.2 Scope

Annual Preventive Maintenance will be performed during standard business hours, unless otherwise agreed to in writing. After the service starts, if the system or Customer requirements dictate that the

service must occur outside of standard business hours, an additional quotation will be provided. The Customer is responsible for any charges associated with unusual access requirements or expenses.

4.1.9.3 Inclusions

Annual Preventive Maintenance service will be delivered for Motorola-provided infrastructure, including integrated third-party products, per the level of service marked in Table 4-17: Preventive Maintenance Level.

Table 4-17: Preventive Maintenance Level

Service Level	Included
Level 1 Preventive Maintenance	X
Level 2 Preventive Maintenance	

Motorola Responsibilities

- Notify the Customer of any planned system downtime needed to perform this service.
- Maintain communication with the Customer as needed until completion of the Annual Preventive Maintenance.
- Determine, in its sole discretion, when an incident requires more than the Annual Preventive Maintenance services described in this SOW, and notify the Customer of an alternative course of action.
- Provide the Customer with a report in Customer Hub, or as otherwise agreed in the CSP, comparing system performance with expected parameters, along with any recommended actions. Time allotment for report completion is to be mutually agreed.
- Provide trained and qualified personnel with proper security clearance required to complete Annual Preventive Maintenance services.
- Field service technician will perform the following on-site:
- Perform the tasks defined in Section 4.1.9.4: Preventative Maintenance Tasks.
  - Perform the procedures defined in Section 4.1.9.5: Site Performance Evaluation Procedures for each site type on the system.
  - Provide diagnostic and test equipment necessary to perform the Preventive Maintenance service.
  - As applicable, use the Method of Procedure (MOP) defined for each task.

Limitations and Exclusions

The following activities are outside the scope of the Annual Preventive Maintenance service.

- Preventive maintenance for third-party equipment not sold by Motorola as part of the original system.
- Network transport link performance verification.
- Verification or assessment of Information Assurance.
- Any maintenance and/or remediation required as a result of a virus or unwanted cyber intrusion.
- Tower climbs, tower mapping analysis, or tower structure analysis.

Customer Responsibilities

- Provide preferred schedule for Annual Preventative Maintenance to Motorola.
- Authorize and acknowledge any scheduled system downtime.
- Maintain periodic backup of databases, software applications, and firmware.
- Establish and maintain a suitable environment (heat, light, and power) for the equipment location as described in equipment specifications, and provide Motorola full, free, and safe access to the equipment so that Motorola may provide services. All sites shall be accessible by standard service vehicles.
- Submit timely changes in any information supplied in the CSP to the CSM.
- Provide site escorts, if required, in a timely manner.
- Provide Motorola with requirements necessary for access to secure facilities.
- In the event that Motorola agrees in writing to provide supplemental Annual Preventive Maintenance to third-party elements provided by Customer, the Customer agrees to obtain any third-party consents or licenses required to enable Motorola field service technician to access the sites to provide the service.

4.1.9.4 Preventative Maintenance Tasks

The Preventive Maintenance service includes the tasks listed in this section. Tasks will be performed based on the level of service noted in Section 4.1.9.3: Inclusions.

PRIMARY SITE CHECKLIST – LEVEL 1	
Servers	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Network Management (NM) Client Applications	Review Unified Event Manager (UEM) events and verify backhaul links are reported as operational. Review event log for persistent types. Verify all NM client applications are operating correctly.
Verify System software physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Complete Backup	Verify backups have been completed or scheduled, and that data has been stored in accordance with the Customer's backup plan. Check that adequate storage space is available for backups.
Network Time Protocol (NTP)	Verify operation and syncing all devices.
Data Collection Devices (DCD) check (if present)	Verify data collection.
Anti-Virus	Verify anti-virus is enabled and that definition files on the core security management server were updated within two weeks of the current date.

PRIMARY SITE CHECKLIST – LEVEL 1	
Routers	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on router type. Capture available diagnostic logs.
Verify Redundant Routers	Test redundancy in cooperative WAN routers. Carry out core router switchover in coordination with Customer.
Switches	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on switch type. Capture available diagnostic logs.
Verify Redundant Switches	Test redundancy in backhaul switches. Carry out core router switchover in coordination with Customer.
Domain Controllers (non-Common Server Architecture)	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Verify System software physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Firewalls	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Logging Equipment	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Server CPU Health	Check memory, HDD, CPU, and disk space utilization.
Software	
Verify System software physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Switches	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Switches (continued)	
Capture Diagnostics	Perform recommended diagnostic tests based on switch type. Capture available diagnostic logs.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.

PRIMARY SITE CHECKLIST – LEVEL 1	
Routers	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on router type. Capture available diagnostic logs.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.
Miscellaneous Equipment	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Site Frequency Standard Check (Timing Reference Unit)	Check LEDs for proper operation.
Site Controllers	
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.
Site Controller Redundancy (Trunking)	Roll site controllers with no dropped audio.
Comparators	
Equipment Alarms	Verify no warning/alarm indicators.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.

DISPATCH SITE CHECKLIST – LEVEL 1	
General	
Inspect all Cables	Inspect all cables and connections to external interfaces are secure.
Mouse and Keyboard	Verify operation of mouse and keyboard.
Configuration File	Verify each operator position has access to required configuration files.
Console Operator Position Time	Verify console operator position time is consistent across all operator positions.
Screensaver	Verify screensaver set as Customer prefers.

DISPATCH SITE CHECKLIST – LEVEL 1	
Screen Performance	Verify screen operational and is not suffering from dead pixels or image burn-in that prevent user operation.
Touchscreen	Verify touchscreen operation, if present.
Cabling/Lights/Fans	Visual inspection of all equipment cabling, lights, and fans
Filters/Fans/Dust	Clean all equipment filters and fans and remove dust.
Monitor and Hard Drive	Confirm the monitor and hard drive do not "sleep".
DVD/CD	Verify and clean DVD or CD drive.
Time Synchronization	Verify console time is synchronized with NTP server
Anti-Virus	Verify anti-virus is enabled and that definition files have been updated within two weeks of the current date.
Headset Unplugged Testing	
Speakers	Test all speakers for audio quality, volume, static, drop-outs, and excess hiss when turned up.
Channel Audio in Speaker	Verify selected channel audio in select speaker only.
Footswitch Pedals	Verify both footswitch pedals operational.
Radio On-Air Light	Verify radio on-air light comes on with TX (if applicable).
Headset Plugged In Testing	
Radio TX and RX	Verify radio TX/RX from both headset jacks. Verify levels OK. Check volume controls for noise, static, or drop-outs.
Speaker Mute	Verify speaker mutes when muted.
Telephone Operation	Verify telephone operational through both headset jacks. Check volume controls for noise, static, or drop-outs.
Audio Switches	Verify audio switches to speaker when phone off-hook if interfaced to phones.
Radio Takeover in Headset	Verify radio-takeover in headset mic when phone is off-hook, with mic switching to radio and muting phone during push-to-talk.

DISPATCH SITE CHECKLIST – LEVEL 1	
Other Tests	
Phone Status Light	Verify phone status light comes on when phone is off-hook (if applicable).
Desk Microphone Operation	Confirm desk mic operation (if applicable).
Radio Instant Recall Recorder (IRR) Operation	Verify radio IRR operational on Motorola dispatch (if applicable).

DISPATCH SITE CHECKLIST – LEVEL 1	
Telephone IRR Operation	Verify telephone IRR operational on Motorola dispatch, if on radio computer.
Recording	Verify operator position being recorded on long term logging recorder, if included in service agreement
Computer Performance Testing	
Computer Reboot	Reboot operator position computer.
Computer Operational	Confirm the client computer is fully operational (if applicable).
Audio Testing	
Conventional Resources	Confirm all conventional resources are functional, with adequate audio levels and quality.
Secure Mode	Confirm any secure talkgroups are operational in secure mode.
Trunked Resources	Confirm all trunked resources on screen are functioning by placing a call in both directions, at the Customer's discretion, and at a single operator position
Backup Resources	Confirm backup resources are operational.
Logging Equipment Testing	
Recording - AIS Test	Verify audio logging of trunked calls.
Recording	With Customer assistance, test operator position logging on recorder.
System Alarms	Review the alarm system on all logging equipment for errors.
Capture Diagnostics	Perform recommended diagnostic tests based on equipment, and capture available diagnostic logs.
Verify System software Physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Playback Station (Motorola Provided)	
Capture Diagnostics	Perform recommended diagnostic tests based on equipment, and capture available diagnostic logs.
Recall Audio	Verify that radio and telephone audio can be recalled.

RF SITE CHECKLIST – LEVEL 1	
RF PM Checklist	
Equipment Alarms	Verify no warning or alarm indicators. Verify AC/DC converter, RMC have been wired correctly on D series site.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.
Site Frequency Standard Check	Check LEDs for proper operation, PCA screens indicating potential faults for proper operation

RF SITE CHECKLIST – LEVEL 1	
Basic Voice Call Check	Voice test each voice path, radio to radio.
Trunking Control Channel Redundancy	Roll control channel, test, and roll back if the site has GTR stations. This test is not applicable for D series stations.
Trunking Site Controller Redundancy, ASTRO 25 Site Repeater only	Roll site controllers with no dropped audio if the site has GTR stations. This test is not applicable for D series stations.
PM Optimization Workbook (See Section 4.1.9.5: Site Performance Evaluation Procedures for GTR tests)	Complete Base Station Evaluation tests - Frequency Error, Modulation Fidelity, Forward at Set Power, Reverse at Set Power, and Gen Level Desense no TX. Update station logs.

MOSCAD CHECKLIST – LEVEL1	
MOSCAD Server	
Equipment Alarms	Verify no warning or alarms indicators.
Check Alarm/Event History	Review MOSCAD alarm and events to find if there are chronic issues.
Windows Event Logs	Review Windows event logs. Save and clear if full.
Password Verification	Log in to site devices to verify passwords. Document changes if any found.
MOSCAD Client	
Equipment Alarms	Verify no warning or alarm indicators.
Check Alarm / Event History	Review MOSCAD alarms and events to find if there are chronic issues.
Windows Event Logs	Review Windows event logs. Save and clear if full.
Password Verification	Site devices to verify passwords. Document changes if any found.
MOSCAD Client (continued)	
Verify System software Physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
MOSCAD RTUs	
Equipment Alarms	Verify no warning or alarm indicators.

MOSCAD CHECKLIST – LEVEL1	
Verify Connectivity	Verify connectivity
Password Verification	Site devices to verify passwords. Document changes if any are found.
Check Alarm/Event History	Review MOSCAD alarms and events to find if there are chronic issues.
Verify System software Physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.

FACILITIES CHECKLIST – LEVEL 1	
Visual Inspection Exterior	
Antenna Site Registration Sign	Verify that the Antenna Site Registration sign is posted.
Warning Sign - Tower	Verify that a warning sign is posted on the tower.
Warning Sign - Gate	Verify that a warning sign is posted at the compound gate entrance.
10 Rule Sign	Verify that a 10 rules sign is posted on the inside of the shelter door.
Outdoor Lighting	Verify operation of outdoor lighting and photocell.
Exterior of Building	Check the exterior of the building for damage and disrepair.
Fences / Gates	Check fences and gates for damage and disrepair.
Landscape / Access Road	Check the landscape and access road for accessibility.
Visual Inspection Interior	
Electrical Surge Protectors	Check electrical surge protectors for alarms.
Emergency Lighting	Verify emergency lighting operation.
Indoor Lighting	Verify indoor lighting.
Equipment Inspection	Visually inspect that all hardware, including equipment, cables, panels, batteries, and racks, is in acceptable physical condition for normal operation.
Visual Inspection Interior (continued)	
Regulatory Compliance (License, ERP, Frequency, Deviation)	Check for site and station FCC licensing indicating regulatory compliance.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.

FACILITIES CHECKLIST – LEVEL 1	
UPS	
Visual inspection (condition, cabling)	Check for damage, corrosion, physical connections, dirt and dust, and error indications.
Generator	
Visual Inspection	Check panel housing for cracks, rust, and weathering. Check physical connections for corrosion, dirt and dust, or other abnormal conditions.
Fuel	Verify fuel levels in backup generators, document date of last fuel delivered from fuel service provider.
Oil	Check the oil dipstick for the proper level. Note the condition of oil.
Verify operation (no switchover)	Verify generator running and check ease or difficulty of start. Is the generator "throttling" or running smooth? Any loud unusual noise? Document any concerns or abnormal conditions.
Motorized Dampers	Check operation
HVAC	
Air Filter	Check air filter and recommend replacement if required.
Coils	Check coils for dirt and straightness.
Outdoor Unit	Check that the outdoor unit is unobstructed.
Wiring	Check wiring for insect and rodent damage.
Cooling / Heating	Check each HVAC unit for cooling/heating.
Motorized Dampers	Check operation.

MICROWAVE CHECKLIST – LEVEL 1	
General	
Transport Connectivity	Confirm transport performance by viewing UEM for site link warnings or errors.
Backhaul Monitoring	Monitor UEM status, including alarms, logs, and events, for all links. If UEM is not used to monitor microwaves, then use an approved vendor-provided microwave alarm management server.
Radio	
Alarms	Check alarm and event history.
Software	Verify version of application.
Radio (continued)	
TX Frequency	Verify transmit frequency.
TX Power	Verify transmit power.
RX Frequency	Verify receive frequency.
RX Signal Level	Verify receive signal level and compare with install baseline documentation.

MICROWAVE CHECKLIST – LEVEL 1	
Save configuration	Save current configuration for off-site storage.
Waveguide	
Visual Inspection	Inspect for wear or dents from ground using binoculars.
Connection Verification	Verify all connections are secured with proper hardware from ground using binoculars.
Dehydrator	
Visual Inspection	Inspect the moisture window for proper color.
Pressure Verification	Verify pressure of all lines.
Re-Pressurization	Bleed lines temporarily to verify the dehydrator re-pressurizes.
Run Hours	Record number of hours ran.

TOWER CHECKLIST – LEVEL 1	
Structure Condition	
Rust	Check the structure for rust.
Cross Members	Check for damaged or missing cross members.
Safety Climb	Check safety climb for damage.
Ladder	Verify that the ladder system is secured to the tower.
Welds	Check for cracks or damaged welds.
Outdoor lighting/photocell	Test outdoor lighting and photocell.
Drainage Holes	Check that drainage holes are clear of debris.
Paint	Check the paint condition.
Tower Lighting	
Lights/Markers	Verify all lights and markers are operational.
Day/Night Mode	Verify day and night mode operation.
Power Cabling	Verify that power cables are secured to the tower.
Antennas and Lines	
Antennas	Visually inspect antennas for physical damage from ground using binoculars.
Transmission Lines	Verify that all transmission lines are secure on the tower.
Grounding	
Structure Grounds	Inspect grounding for damage or corrosion
Guy Wires	
Tower Guys	Visually inspect guy wires for fraying, loss of tension, or loss of connection.
Guy Wire Hardware	Check hardware for rust.

TOWER CHECKLIST – LEVEL 1	
Concrete Condition	
Tower Base	Check for chips or cracks.

PRIMARY SITE CHECKLIST – LEVEL 2	
Servers	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Network Management (NM) Client Applications	Review Unified Event Manager (UEM) events and verify backhaul links are reported as operational. Review event log for persistent types. Verify all NM client applications are operating correctly.
Verify System software physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Complete Backup	Verify backups have been completed or scheduled, and that data has been stored in accordance with the Customer's backup plan. Check that adequate storage space is available for backups.
Network Time Protocol (NTP)	Verify operation and syncing all devices.
Data Collection Devices (DCD) check (if present)	Verify data collection.
Anti-Virus	Verify anti-virus is enabled and that definition files on the core security management server were updated within two weeks of current date.
Verify Software	Verify that the latest MOTOPATCH, released for Microsoft Windows by Motorola, has been installed.
Verify Redundant Zone Controllers (ZC)	Perform ZC switchover. Coordinate with Customer to switch from ZC1 to ZC2 and back again.
Active Directory	Verify directory by running domain controller diagnostics (dcdiag), domain replication test (repadmin), and DNS diagnostics utility (dnslint).

PRIMARY SITE CHECKLIST – LEVEL 2	
Routers	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on router type. Capture available diagnostic logs.
Verify Redundant Routers	Test redundancy in cooperative WAN routers. Carry out core router switchover in coordination with Customer.

PRIMARY SITE CHECKLIST – LEVEL 2	
Switches	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on switch type. Capture available diagnostic logs.
Verify Redundant Switches	Test redundancy in backhaul switches. Carry out core router switchover in coordination with Customer.
Domain Controllers (non-Common Server Architecture)	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Verify System software physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Firewalls	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Logging Equipment	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Server CPU Health	Check memory, HDD, CPU, and disk space utilization.
Software	
Verify System software physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Verify System software Installed	Verify software versions installed on the system. Document any changes.
Switches	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on switch type. Capture available diagnostic logs.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.
Verify Redundant Switches	Test redundancy in backhaul switches. Carry out core router switchover in coordination with Customer.
Routers	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.

PRIMARY SITE CHECKLIST – LEVEL 2	
Capture Diagnostics	Perform recommended diagnostic tests based on router type. Capture available diagnostic logs.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.
Verify Redundant Routers	Test redundancy in cooperative WAN routers. Carry out core router switchover in coordination with Customer.
Miscellaneous Equipment	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Site Frequency Standard Check (Timing Reference Unit)	Check LEDs for proper operation.
Site Controllers	
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.
Site Controller Redundancy (Trunking)	Roll site controllers with no dropped audio.
Verify Software	Verify that the latest MOTOPATCH, released for Microsoft Windows by Motorola, has been installed.
Comparators	
Equipment Alarms	Verify no warning/alarm indicators.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.

DISPATCH SITE CHECKLIST – LEVEL 2	
General	
Inspect all Cables	Inspect all cables and connections to external interfaces are secure.
Mouse and Keyboard	Verify operation of mouse and keyboard.
Configuration File	Verify each operator position has access to required configuration files.
Console Operator Position Time	Verify console operator position time is consistent across all operator positions.

DISPATCH SITE CHECKLIST – LEVEL 2	
Screensaver	Verify screensaver set as Customer prefers.
Screen Performance	Verify screen operational and is not suffering from dead pixels or image burn-in that prevent user operation.
Touchscreen	Verify touchscreen operation, if present.
Cabling/Lights/Fans	Visual inspection of all equipment cabling, lights, and fans
Filters/Fans/Dust	Clean all equipment filters and fans and remove dust.
Monitor and Hard Drive	Confirm the monitor and hard drive do not "sleep".
DVD/CD	Verify and clean DVD or CD drive.
Time Synchronization	Verify console time is synchronized with NTP server
Anti-Virus	Verify anti-virus is enabled and that definition files have been updated within two weeks of the current date.
Headset Unplugged Testing	
Speakers	Test all speakers for audio quality, volume, static, drop-outs, and excess hiss when turned up.
Channel Audio in Speaker	Verify selected channel audio in select speaker only.
Footswitch Pedals	Verify both footswitch pedals operational.
Radio On-Air Light	Verify radio on-air light comes on with TX (if applicable).
Headset Plugged In Testing	
Radio TX and RX	Verify radio TX/RX from both headset jacks. Verify levels OK. Check volume controls for noise, static, or drop-outs.
Speaker Mute	Verify speaker mutes when muted.
Telephone Operation	Verify telephone operational through both headset jacks. Check volume controls for noise, static, or drop-outs.
Audio Switches	Verify audio switches to speaker when phone off-hook if interfaced to phones.
Radio Takeover in Headset	Verify radio-takeover in headset mic when phone is off-hook, with mic switching to radio and muting phone during push-to-talk.

DISPATCH SITE CHECKLIST – LEVEL 2	
Other Tests	
Phone Status Light	Verify phone status light comes on when phone is off-hook (if applicable).
Desk Microphone Operation	Confirm desk mic operation (if applicable).

DISPATCH SITE CHECKLIST – LEVEL 2	
Radio Instant Recall Recorder (IRR) Operation	Verify radio IRR operational on Motorola dispatch (if applicable).
Telephone IRR Operation	Verify telephone IRR operational on Motorola dispatch, if on radio computer.
Recording	Verify operator position being recorded on long term logging recorder, if included in service agreement
IRR Setup Parameters	Check IRR set-up parameters, audio card set-up, and level adjustments.
Paging Controls	Confirm all paging controls are functional, including third-party encoders if covered by maintenance contract.
Computer Performance Testing	
Computer Reboot	Reboot operator position computer.
Computer Operational	Confirm the client computer is fully operational (if applicable).
Event Logs	Pull event logs and review for major errors.
Hard Drive Backup	Create backup of drive for offsite storage.
Memory Usage	Check memory usage.
Application Logs and Alerts	Review built in application logs and alerts.
Hard Drive Usage	Check available space, ensure there is a minimum of 10%.
Verify Software	Verify that the latest MOTOPATCH, released for Microsoft Windows by Motorola, has been installed.
Audio Testing	
Conventional Resources	Confirm all conventional resources are functional, with adequate audio levels and quality.
Secure Mode	Confirm any secure talkgroups are operational in secure mode.
Trunked Resources	Confirm all trunked resources on screen are functioning by placing a call in both directions, at the Customer's discretion, and at a single operator position
Backup Resources	Confirm backup resources are operational.
Paging Tones	Confirm tone sequences and paging operations.

DISPATCH SITE CHECKLIST – LEVEL 2	
Logging Equipment Tests	
Recording - AIS Test	Verify audio logging of trunked calls.
Recording	With Customer assistance, test operator position logging on recorder.
System Alarms	Review the alarm system on all logging equipment for errors.

DISPATCH SITE CHECKLIST – LEVEL 2	
Capture Diagnostics	Perform recommended diagnostic tests based on equipment, and capture available diagnostic logs.
Verify System software Physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Verify Software	Verify that the latest MOTOPATCH, released for Microsoft Windows by Motorola, has been installed.
Playback Station (Motorola Provided)	
Capture Diagnostics	Perform recommended diagnostic tests based on equipment, and capture available diagnostic logs.
Recall Audio	Verify that radio and telephone audio can be recalled.

RF SITE CHECKLIST – LEVEL 2	
RF PM Checklist	
Equipment Alarms	Verify no warning or alarm indicators.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.
Site Frequency Standard Check	Check LEDs for proper operation, PCA screens indicating potential faults for proper operation.
Basic Voice Call Check	Voice test each voice path, radio to radio.
Trunking Control Channel Redundancy	Roll control channel, test, and roll back if the site has GTR stations. This test is not applicable for D series stations.
Trunking Site Controller Redundancy, ASTRO 25 Site Repeater only	Roll site controllers with no dropped audio if the site has GTR stations. This test is not applicable for D series stations.
PM Optimization Workbook (See Section 4.1.9.5: Site Performance Evaluation Procedures for GTR tests)	Complete Base Station Evaluation tests - Frequency Error, Modulation Fidelity, Forward at Set Power, Reverse at Set Power, and Gen Level Desense no TX. Update station logs.

MOSCAD CHECKLIST – LEVEL 2	
MOSCAD Server	
Equipment Alarms	Verify no warning or alarm indicators.

MOSCAD CHECKLIST – LEVEL 2	
Check Alarm/Event History	Review MOSCAD alarms and events to find if there are chronic issues.
Windows Event Logs	Review Microsoft Windows event logs. Save and clear if full.
Password Verification	Log in to site devices to verify passwords. Document changes if any are found.
Verify System software Physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Verify Software	Verify that the latest MOTOPATCH, released for Microsoft Windows by Motorola, has been installed.
Server CPU Health	Check memory, HDD, CPU, and disk space utilization.
Verify System software Installed	Verify software versions installed on the system. Document any changes.
MOSCAD Client	
Equipment Alarms	Verify no warning or alarm indicators.
Check Alarm / Event History	Review MOSCAD alarms and events to find if there are chronic issues.
Windows Event Logs	Review Microsoft Windows event logs. Save and clear if full.
Password Verification	Site devices to verify passwords. Document changes if any are found.
Verify System software Physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Verify Software	Verify that the latest MOTOPATCH, released for Microsoft Windows by Motorola, has been installed.
MOSCAD RTUs	
Equipment Alarms	Verify no warning or alarm indicators.
Verify Connectivity	Verify connectivity
Password Verification	Site devices to verify passwords. Document changes if any are found.
Check Alarm/Event History	Review MOSCAD alarms and events to find if there are chronic issues.
Verify System software Physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to the Customer server.
Verify System software Installed	Verify software versions installed on the system. Document any changes.

FACILITIES CHECKLIST – LEVEL 2	
Visual Inspection Exterior	
Antenna Site Registration Sign	Verify that the Antenna Site Registration sign is posted.
Warning Sign - Tower	Verify that a warning sign is posted on the tower.
Warning Sign - Gate	Verify that a warning sign is posted at the compound gate entrance.
10 Rule Sign	Verify that a 10 rules sign is posted on the inside of the shelter door.
Outdoor Lighting	Verify operation of outdoor lighting and photocell.
Exterior of Building	Check the exterior of the building for damage and disrepair.
Fences / Gates	Check fences and gates for damage and disrepair.
Landscape / Access Road	Check the landscape and access road for accessibility.
Visual Inspection Interior	
Electrical Surge Protectors	Check electrical surge protectors for alarms.
Emergency Lighting	Verify emergency lighting operation.
Indoor Lighting	Verify indoor lighting.
Equipment Inspection	Visually inspect that all hardware, including equipment, cables, panels, batteries, and racks, is in acceptable physical condition for normal operation.
Regulatory Compliance (License, ERP, Frequency, Deviation)	Check for site and station FCC licensing indicating regulatory compliance.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.
UPS	
Visual inspection (condition, cabling)	Check for damage, corrosion, physical connections, dirt and dust, and error indications.
Rollover and Rollback of UPS and Generator	Verify automatic switch to backup power when main power fails.
Battery voltage checks	Verify, check and measure battery voltages.
Generator	
Visual Inspection	Check panel housing for cracks, rust, and weathering. Check physical connections for corrosion, dirt and dust, or other abnormal conditions.
Fuel	Verify fuel levels in backup generators, document date of last fuel delivered from fuel service provider.

FACILITIES CHECKLIST – LEVEL 2	
Oil	Check the oil dipstick for the proper level. Note the condition of oil.
Verify operation (no switchover)	Verify generator running and check ease or difficulty of start. Is the generator "throttling" or running smooth? Any loud unusual noise? Document any concerns or abnormal conditions.
Motorized Dampers	Check operation
Verify rollover and rollback	Verify automatic switch to backup power when main power fails.
HVAC	
Air Filter	Check the air filter and recommend replacement if required.
Coils	Check coils for dirt and straightness.
Outdoor Unit	Check that the outdoor unit is unobstructed.
Wiring	Check wiring for insect and rodent damage.
Cooling / Heating	Check each HVAC unit for cooling/heating.
Motorized Dampers	Check operation.

MICROWAVE CHECKLIST – LEVEL 2	
General	
Transport Connectivity	Confirm transport performance by viewing UEM for site link warnings or errors.
Backhaul Monitoring	Monitor UEM status, including alarms, logs, and events, for all links. If UEM not used to monitor microwaves, then use an approved vendor-provided microwave alarm management server.
Radio	
Alarms	Check alarm and event history.
Software	Verify version of application.
TX Frequency	Verify transmit frequency.
TX Power	Verify transmit power.
RX Frequency	Verify receive frequency.
RX Signal Level	Verify receive signal level and compare with install baseline documentation.
Save configuration	Save current configuration for off-site storage.
Waveguide	
Visual Inspection	Inspect for wear or dents from ground using binoculars.
Connection Verification	Verify all connections are secured with proper hardware from ground using binoculars.
Dehydrator	
Visual Inspection	Inspect the moisture window for proper color.

MICROWAVE CHECKLIST – LEVEL 2	
Pressure Verification	Verify pressure of all lines.
Re-Pressurization	Bleed lines temporarily to verify the dehydrator re-pressurizes.
Run Hours	Record number of hours ran.

TOWER CHECKLIST – LEVEL 2	
Structure Condition	
Rust	Check the structure for rust.
Cross Members	Check for damaged or missing cross members.
Safety Climb	Check safety climb for damage.
Ladder	Verify that the ladder system is secured to the tower.
Welds	Check for cracks or damaged welds.
Outdoor lighting/photocell	Test outdoor lighting and photocell.
Drainage Holes	Check that drainage holes are clear of debris.
Paint	Check the paint condition.
Tower Lighting	
Lights/Markers	Verify all lights and markers are operational.
Day/Night Mode	Verify day and night mode operation.
Power Cabling	Verify that power cables are secured to the tower.
Antennas and Lines	
Antennas	Visually inspect antennas for physical damage from ground using binoculars.
Transmission Lines	Verify that all transmission lines are secure on the tower.
Grounding	
Structure Grounds	Inspect grounding for damage or corrosion
Guy Wires	
Tower Guys	Visually inspect guy wires for fraying, loss of tension, or loss of connection.
Guy Wire Hardware	Check hardware for rust.
Concrete Condition	
Tower Base	Check for chips or cracks.

4.1.9.5 Site Performance Evaluation Procedures

The Preventive Maintenance service includes the site performance evaluation procedures listed in this section.

ASTRO 25 GTR ESS SITE PERFORMANCE
Antennas
Transmit Antenna Data
Receive Antenna System Data
Tower Top Amplifier Data
FDMA Mode
Base Radio Transmitter Tests
Base Radio Receiver Tests
Base Radio Transmit RFDS Tests
Receive RFDS Tests with TTA (if applicable)
Receive RFDS Tests without TTA (if applicable)
TDMA Mode
Base Radio TDMA Transmitter Tests
Base Radio TDMA Receiver Tests
TDMA Transmit RFDS Tests
TDMA Receive RFDS Tests with 432 Diversity TTA
TDMA Receive RFDS Tests with 2 Independent TTA's (if applicable)
TDMA Receive RFDS Tests without TTA (if applicable)

4.1.10 Microwave and MPLS Tested Vendor Product Monitoring-(Not Included)

Microwave and MPLS Tested Vendor Product Monitoring provides continuous real-time “endpoint” event monitoring, directing the Customer’s attention to potential disruptions to new or existing individual ASTRO 25 backhaul elements, such as MPLS routers and microwave radios.

4.1.10.1 Description of Service

Motorola’s Microwave and MPLS Tested Vendor Product Monitoring service provides real-time “endpoint” event monitoring of backhaul links. Microwave and MPLS Tested Vendor Product Monitoring uses sophisticated tools for remote detection and classification of events on the Customer’s backhaul network. Select third-party network elements from vendors such as Nokia, Juniper, Aviat, and MNI, are integrated into Motorola’s event management system, as referenced in Table 4-18: Standard Monitored Backhaul Network Elements. When an event is detected, Motorola will determine the status of the impacted backhaul element and dispatch the Field Service Technician (Servicer) to respond to and remediate the issue.

Microwave and MPLS Tested Vendor Product Monitoring aims to reduce or avoid network downtime through three elements:

- Simplifying the remediation process for lost critical and redundant site links, so any downtime from failure is reduced by monitoring the endpoints of the links and detecting indications that a failure has occurred.
- Setting the right rules and thresholds, so “False Positive Events” can be avoided on the path bounces, identifying which events need to be addressed.

4.1.10.2 Scope

Motorola monitors the status of the Customer’s site connectivity 24 hours a day, seven days a week via ASTRO 25 backhaul network elements. Motorola’s tools and processes for monitoring ASTRO 25 radio networks will be leveraged to monitor the backhaul endpoint.

Motorola defines detected events based on what backhaul elements they impact. Motorola monitors for the following types of incidents:

- Loss of primary or redundant link.
- Failed site information.
- Physical link degradation information.
- Failure of the Microwave radio, MPLS router, or a subcomponent of either.

When an event is detected and classified, Motorola will notify and dispatch the Customer’s Servicer to resolve the issue.

4.1.10.3 Prerequisites

- 7.17.3 ASTRO 25 System release or beyond.
- ASTRO 25 Network Event Monitoring Service.
- Existing or newly procured Microwave or MPLS equipment with relevant spares. Refer to Table 4-18: Standard Monitored Backhaul Network Elements for a list of supported backhaul elements.
- The latest approved and configured model of the Motorola Backhaul Management Firewall.
- Equipment to be monitored is of the minimum firmware/software version to support the required Simple Network Management Protocol (SNMP) implementation for Unified Endpoint Management (UEM) integration.
- In some cases, a proxy application is required between the network element and UEM (such as Aviat ProVision). This must be procured by the customer and have the appropriate software version and feature license.

4.1.10.4 Inclusions

Microwave and MPLS Tested Vendor Product Monitoring is available for the primary and redundant backhaul links within the Customer’s ASTRO 25 radio network.

Motorola Responsibilities

- Use concurrent connectivity through the network connection established to support Network Event Monitoring.

- Verify connectivity and event monitoring prior to system acceptance or start date.
- Monitor backhaul link endpoints continuously 24 hours per day, 7 days per week.
- Create incident tickets, when necessary, in accordance with Section 4.1.10.6: Microwave and MPLS Tested Vendor Product Monitoring Priority Level Definitions and Response Times. Identify and classify the link associated with the incident.
- Dispatch the Customer's Servicer when necessary and maintain communications with the Customer until the incident is resolved. Provide updates in accordance with the agreed frequency documented in the CSP, until resolution.
- Motorola's CSM shall validate quotes and execute separately procured third-party maintenance contracts.
- Motorola's Field or Network Solution Architects may provide initial configuration or provisioning assistance to enable this service.

Limitations and Exclusions

- The Microwave and MPLS Tested Vendor Product Monitoring service is limited to monitoring the individual backhaul elements, as listed in Table 4-18: Standard Monitored Backhaul Network Elements, within the ASTRO 25 radio network where the primary and redundant backhaul links terminate.
- This service does not include Network Element Repair, Replacement, or Remote Technical Support. The Customer will be responsible to acquire a maintenance contract from the tested vendors or Motorola.
- Motorola is not responsible for system performance faults or deficiencies that are caused by changes or modifications to the system not performed by Motorola.
- Motorola reserves the right to adjust the price of the Microwave and MPLS Tested Vendor Product Monitoring service if it is found that the Customer's backhaul network exhibits excessive demand due to:
  - Out of Support and/or End of Life (EOL) backhaul equipment.
  - The Customer and/or backhaul vendor has made changes to the backhaul network outside the agreed Change Management process.
- Microwave and MPLS Tested Vendor Product Monitoring is available for ASTRO 25 systems at release 7.17.3 or later, in the United States and Canada only.
- New backhaul elements or backhaul elements that undergo significant software changes or upgrades require a minimum of 28 days to incorporate into Microwave and MPLS Tested Vendor Product Monitoring Service.

Customer Responsibilities

- Provide Motorola with continuous remote access to enable the monitoring service.
- If the network element requires a software or firmware upgrade to address an issue that affects this service, the customer shall be responsible for the procurement and upgrade.
- Prior to the start of service, provide Motorola with pre-defined customer information and preferences necessary to complete the CSP, including:
  - Name and contact information of the Servicer under contract.
  - Obtain permission for Motorola to act on the Customer's behalf to contact the Customer's Servicer and dispatch such Servicer to respond to events.

  - Coordinate testing between the Customer's transmission supplier, Servicer, and Motorola prior to operational acceptance.
  - Keep the Customer's backhaul network up to date, applying recent patches and replacing unsupported backhaul elements as needed.
  - Submit timely changes in any information supplied to Motorola and included in the CSP to the CSM and in accordance with the Change Management process.
  - Act as a point of escalation for Motorola in the event the backhaul Servicer(s) is, in Motorola's reasonable opinion, unresponsive, slow to respond, or lacks the urgency or capability to resolve incidents.
- Notify Motorola, in accordance with the Change Management process, when the Customer or Servicer performs any activity that affects the system. Activities that affect the system may include, but are not limited to, installing software or hardware upgrades, performing upgrades to the network, or taking down part of the system to perform maintenance.
- Provide Motorola with accounts and passwords, separate from the Customer's accounts and passwords, to allow Motorola to request service support or initiate a response to a technical issue from the Customer's Servicer.
- Pay additional support charges above and beyond the contracted service rates that may apply if it is determined that system faults were caused by the Customer making changes to critical system parameters.
- Obtain any third-party consents or licenses required to enable Motorola to provide the monitoring service.
- Cooperate with Motorola, and perform acts that are reasonable or necessary to enable Motorola to provide the services described in this SOW.
- Prior to service onboarding, inform Motorola if the Customer needs Microwave and MPLS Tested Vendor Product Monitoring coverage for backhaul elements not listed in Section 4.1.10.5: Monitored Backhaul Network Elements.
  - Provide Motorola with MIB files necessary for Motorola to configure new backhaul elements at least 28 days before monitoring needs to commence.

4.1.10.5 Monitored Backhaul Network Elements

The Microwave and MPLS Tested Vendor Product Monitoring service supports the models listed in Table 4-18: Standard Monitored Backhaul Network Elements. Motorola can configure monitoring for these backhaul elements. To monitor any backhaul elements not listed in this table, the Customer will need to request vetting and approval by Motorola product and services teams prior to service onboarding. A minimum of 28 days is required to vet and configure new backhaul elements using MIB files provided by the Customer.

Table 4-18: Standard Monitored Backhaul Network Elements

Vendor	Model #	Type	Software Version	Release Alignment
Nokia	7705 SAR-8	MPLS Router	TiMOS R8.9 and up	7.17.3 +
Nokia	7705 SAR-18	MPLS Router	TiMOS R8.9 and up	7.17.3 +
Nokia	7705 SAR A	MPLS Router	TiMOS R8.9 and up	7.17.3 +
Nokia	7705 SAR A + T1	MPLS Router	TiMOS R8.9 and up	7.17.3 +

Vendor	Model #	Type	Software Version	Release Alignment
Nokia	7705 SAR M	MPLS Router	TiMOS R8.9 and up	7.17.3 +
Nokia	7705 SAR M + T1	MPLS Router	TiMOS R8.9 and up	7.17.3 +
Nokia	9500 MPR	Microwave Radio	n/a - decoupled	7.17.3 +
Nokia	Wavence	Microwave Radio	n/a - decoupled	7.17.3 +
Nokia	TSM8000	Element Manager	Tsm8k R8	7.17.3 +
Juniper	Juniper MX5	MPLS Router	Junos R15.1 and up	7.17.3 +
Juniper	Juniper MX80	MPLS Router	Junos R15.1 and up	7.17.3 +
Juniper	Juniper MX104	MPLS Router	Junos R15.1 and up	7.17.3 +
Juniper	Juniper MX150	MPLS Router	Junos R15.1 and up	7.17.3 +
Juniper	Juniper MX204	MPLS Router	Junos R15.1 and up	7.17.3 +
Juniper	Juniper ACX1100	MPLS Router	Junos R15.1 and up	7.17.3 +
Aviat	Pro Vision	Element Manager	R 7.8.1.34+	7.17.3 +
Aviat	Eclise Microwave	Microwave Radio	n/a - decoupled	7.17.3 +
Microwave Networks	Proteus-MX, MXD	Microwave Radio	R 3.E	7.17.3 +
NEC	Ipasolink I250, I650	Microwave Radio	Any	7.17.3 +

4.1.10.6 Microwave and MPLS Tested Vendor Product Monitoring Priority Level Definitions and Response Times

Incident Priority	Incident Definition	Initial Response Time
High P2	▪ **Core**: Core server or link failures. Redundant server or link available. ▪ **Consoles**: Between 20% and 40% of a site's console positions down. ▪ **Sites/Subsites**: One RF site or up to 10% of RF sites down, whichever is greater. ▪ **Conventional Channels**: Up to 50% of CCGWs down. Redundant gateways available. ▪ **Network Elements**: Site router, site switch, or GPS server down. No redundant networking element available.	Response provided 24/7 until service restoration. Technical resource will acknowledge incident and respond within 4 hours of CMSO logging incident.
Medium P3	▪ **Consoles**: Up to 20% of a site's console positions down. ▪ **Conventional Channels**: Single channel down. Redundant gateway available. ▪ **Network Elements**: Site router/switch or GPS server down. Redundant networking element available.	Response provided during normal business hours until service restoration. Technical resource will acknowledge incident and respond within 1 Business Day of CMSO logging incident.

Critical P1 and Low P4 incidents do not apply to the Microwave and MPLS Tested Vendor Product Monitoring Service.

Section 5

Priority Level Definitions and Response Times

Table 5-1: Priority Level Definitions and Response Time describes the criteria Motorola uses to prioritize incidents and service requests, and lists the response times for those priority levels.

Table 5-1: Priority Level Definitions and Response Time

Incident Priority	Incident Definition	Initial Response Time	On-Site Response Time
Critical P1	▪ **Core:** Core server or core link failure. No redundant server or link available. ▪ **Sites/Subsites:** Primary site down. Two RF sites or more than 10% of RF sites down, whichever is greater. ▪ **Consoles:** More than 40% of a site's console positions down. ▪ **Conventional Channels:** Conventional Channel Gateways (CCGW) down without redundant gateways available. ▪ **Security Features:** Security is non-functional or degraded. ▪ **Alarm Events:** Door, motion, intrusion, power failure, or environmental alarms triggered.	Response provided 24/7 until service restoration. Technical resource will acknowledge incident and respond within 30 minutes of CMSO logging incident.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
High P2	▪ **Core:** Core server or link failures. Redundant server or link available. ▪ **Consoles:** Between 20% and 40% of a site's console positions down. ▪ **Sites/Subsites:** One RF site or up to 10% of RF sites down, whichever is greater. ▪ **Conventional Channels:** Up to 50% of CCGWs down. Redundant gateways available. ▪ **Network Elements:** Site router, site switch, or GPS server down. No redundant networking element available.	Response provided 24/7 until service restoration. Technical resource will acknowledge incident and respond within 1 hour of CMSO logging incident.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
Medium P3	▪ **Consoles:** Up to 20% of a site's console positions down. ▪ **Conventional Channels:** Single channel down. Redundant gateway available. ▪ **Network Elements:** Site router/switch or GPS server down. Redundant networking element available.	Response provided during normal business hours until service restoration. Technical resource will acknowledge incident and respond within 4 hours of CMSO logging incident.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 8 hours of receiving dispatch notification.

Incident Priority	Incident Definition	Initial Response Time	On-Site Response Time
Low P4	▪ **Service Requests:** Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).	Response provided during normal business hours. Motorola will acknowledge and respond within 1 Business Day.	Not applicable.

Appendix 1: ASTRO 25 Remote Security Update Coverage