Exhibit A

MOTOROLA SOLUTIONS

CHANGE ORDER

Change Order No. 03

Date: 9/3/2020

Project Name: Santa Rosa Police Department-TDMA Infrastructure & Subscribers

Customer Name: Santa Rosa Police Department

Customer Project Mgr: Cheri Lynn Eklund

The purpose of this Change Order is to:

Add Maintenance and System Upgrade (SUA II) program.

Contract # CA-19I177A **Contract Date:** **December 21, 2018**

In accordance with the terms and conditions of the contract identified above between Santa Rosa Police Department and Motorola Solutions, Inc., the following changes are approved:

Contract Price Adjustments

Original Contract Value:	$ 5,303,186.69
Previous Change Order amounts for Change Order numbers 1 through 2	$ 45,402
This Change Order:	2,755,731.11
Contract Credit Amount (DDR changes)	$ 0.00
Reduction in Contract Credit	$ 0.00
Revised Contract Credit Amount	$ 0.00
New Contract Value:	$ 8,104,319.80

Completion Date Adjustments

Original Completion Date:	NA
Current Completion Date prior to this Change Order:	NA
New Completion Date:	NA

MOTOROLA SOLUTIONS

CHANGE ORDER

Changes in Equipment: *(additions, deletions or modifications)*

.
NONE

Changes in Services: *(additions, deletions or modifications)*

The purpose of this change order is to add services, maintenance and system upgrades to the contract.

Schedule Changes: *(describe change or N/A)*

N/A

Pricing Changes: *(describe change or N/A)*

Add 9 years of Maintenance – $1,308,369.00
Add 9 years of SUA II – $1,447,362.11
Total Additional – $2,755,731.11

Statement of Work:

(SEE ATTACHED FOR STATEMENT OF WORK)

Payment Schedule for this Change Order:
(describe new payment terms applicable to this change order)

Description	Maintenance ($)	SUA ($)	Total
Year 1 – April 1, 2021 (Core+Consoles)	$106,874.00	$146,370.52	$253,244.52
Year 2– April 1, 2022 (RF Warranty year)	$110,783.00	$143,468.40	$254,251.40
Year 3– April 1, 2023 (Core+Consoles+RF)	$151,439.00	$157,210.95	$308,649.95
Year 4– April 1, 2024	$157,534.00	$160,044.52	$317,578.52
Year 5*– April 1, 2025	$138,353.00	$162,963.12	$301,316.12
Year 6– April 1, 2026	$145,072.00	$165,967.68	$311,039.68
Year 7– April 1, 2027	$158,242.00	$168,163.32	$326,405.32
Year 8– April 1, 2028	$165,975.00	$170,422.98	$336,397.98
Year 9– April 1, 2029	$174,097.00	$172.750.62	$346,847.62
TOTAL SUA/Maintenance – Years 1-9	**$1,308,369.00**	**$1,447,362.11**	**$2,755,731.11**

Clarifications:
Year 1 includes Maintenance and SUA program for the Core and Consoles provided in Phase 1 of Santa Rosa PD's radio project.

Year 2 continues the Maintenance and SUA for the Core and Consoles. During year 2, the radio sites equipment will be under warranty and supported as part of original contract.

Year 3 will continue the Maintenance and SUA for the Core and Consoles and incorporates the Maintenance and SUA of the radio site equipment as well.

MOTOROLA SOLUTIONS

CHANGE ORDER

Year 5, NOKIA microwave software upgrade and support service is limited to 5 years by the 3rd party vendor and will drop out in 2025. For Lifecycle Support: Motorola will invoice Customer annually in advance of each year of the plan. Customer will make payments to Motorola within thirty (30) days.

Unless amended above, all other terms and conditions of the Contract signed by the parties on December 21, 2018, shall remain in full force. If there are any inconsistencies between the provisions of this Change Order and the provisions of the Contract, the provisions of this Change Order will prevail.

IN WITNESS WHEREOF the parties have executed this Change Order as of the last date signed below.

Motorola, Inc.		**Customer**	
By:	_____	By:	_____
Printed Name:	_____	Printed Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

Reviewed by: Cheri Lynn Eklund Date: 08/07/20
Motorola Project Manager

MOTOROLA SOLUTIONS

CA-19I177A – COR 3 - STATEMENT OF WORK

SANTA ROSA POLICE DEPARTMENT

Change Order 3 – Statement of Work

September 2020

TABLE OF CONTENTS

Contents

Santa Rosa Police Department 1

Section 1 1-1

Advanced Services Statement of Work 1-1

1.1 Introduction 1-1

1.1.1 Advanced Services 1-1

1.1.2 Customer Support Plan (CSP) 1-1

1.1.3 Centralized Service Delivery 1-2

1.1.4 Field Service Delivery 1-2

1.1.5 Network Hardware Repair 1-3

1.1.6 Security Management Operations 1-3

1.1.7 MyView Portal 1-3

1.2 Appendix A: Network Event Monitoring Statement of Work 1-5

1.2.1 Engagement Matrix 1-8

1.2.2 Connectivity Matrix 1-8

1.3 Appendix B: Technical Support Statement of Work 1-11

1.4 Appendix C: Network Hardware Repair Statement of Work 1-16

1.5 Appendix D: Remote Security Patch Installation Statement of Work 1-20

1.6 Appendix E: OnSite Support Statement of Work 1-26

1.7 Appendix F: Annual Preventive Maintenance Statement of Work 1-31

Section 2 1-41

Lifecycle Statement of Work 1-41

2.1 ASTRO 25 System Upgrade Agreement II (SUA II) 1-41

SECTION 1

ADVANCED SERVICES STATEMENT OF WORK

1.1 INTRODUCTION

This Statement of Work (SOW), including all of its subsections and attachments is an integral part of the Services Agreement or other signed agreement between Motorola Solutions, Inc. (Motorola) and Customer ("Agreement") and is subject to the terms and conditions set forth in the Agreement.

Advanced Services are Network Event Monitoring, Technical Support, Network Hardware Repair, Remote Security Patch Installation, OnSite Support and Annual Preventive Maintenance. Each of these services are summarized below and expanded upon in the appendices A, B, C, D, E ,F. In the event of a conflict between the Sections below and an individual SOW Subsection, the individual SOW Subsection prevails.

1.1.1 Advanced Services

Motorola's Advanced Services are designed for customers who would benefit from Motorola's support experience. Advanced Services are delivered through a combination of centralized resources within Motorola's Solutions Support Center (SSC) collaborating with authorized local field services delivery resources that are experienced in managing mission critical networks and associated technologies. The MSI SSC operates 24 x 7 x 365, leveraging field resources that are either dedicated to the network or engaged as needed.

Advanced Services applies to fixed end communications network equipment located at the network core, RF site and dispatch sites. Advanced Services do not include maintenance of mobile or portable devices, or network backhaul.

The services described in this SOW will be performed in accordance with the Customer Support Plan (CSP) agreed upon by the parties.

The CSP will define the system elements covered under Advanced Services. The division of responsibilities between Motorola and Customer shall be defined and documented in the Appendices of this SOW, the Advanced Services CSP and other portions of the Agreement.

1.1.2 Customer Support Plan (CSP)

The Advanced Services Statement of Work summarizes Motorola's delivery approach and standard goals. Since individual customer technologies, systems, operating environments, and operational capabilities differ, the outlined services approach in the Advanced Services SOW will be adapted to each Customer's own environment and unique needs via the CSP.

The CSP is a critical component of this SOW and, once created, will automatically become integrated into this SOW by this reference. Motorola and Customer will collaborate to define

the Customer-specific processes, procedures, network information, and other relevant support details required to perform the Services set forth in the Advanced Services SOW.

1.1.3 Centralized Service Delivery

Network Event Monitoring provides for real time continuous event management for radio communications networks. The SSC Network Operations Center utilizes sophisticated tools for remote monitoring and event characterization of customer communications networks. When an event is detected, technologists acknowledge and assess the situation, and initiate a defined response. Appendix A contains the SOW for Network Event Monitoring.

Technical Support provides telephone consultation for technical issues that require a high level of ASTRO 25 network experience and troubleshooting capabilities. Technical Support is delivered through the Motorola Solutions Support Center (SSC) 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, reflecting the importance of maintaining mission critical systems. Appendix B contains the SOW for Technical Support.

The Service Desk provides a single point of contact for all Service related items, including communications between Customer, Third-Party Subcontractors, and Motorola. The Service Desk provides an ingress/egress point for Service Requests, Service Incidents, Changes, and Dispatch. All incoming transactions through the Service Desk are recorded, tracked and updated through the Motorola Customer Relationship Management (CRM) system. Key responsibilities are: Documentation of customer inquiries, requests, concerns and related tickets. Tracking and resolution of issues, and timely communication with all stakeholders is based on the nature of the incident and the requirements of the CSP. The Services Desk will manage service requests received from authorized parties and will coordinate the appropriate response with Customer and third parties, as necessary.

1.1.4 Field Service Delivery

Advanced Services are provided by authorized local field Services delivery resources. Annual Preventive Maintenance and OnSite Support are both managed from the SSC, but delivered by authorized local field services resources.

OnSite Support provides local, trained and qualified technicians who arrive at the customer location upon a dispatch service call to diagnose and restore the communications network. This involves running diagnostics on the hardware or FRU (Field Replacement Unit) and replacing defective infrastructure or FRU. The system technician will respond to the customer location based on pre-defined Incident priority levels. Appendix E contains the SOW for Onsite Support.

Annual Preventive Maintenance Service provides proactive, regularly scheduled operational test and alignment of infrastructure and network components to continually meet original manufacturer's specifications. Certified field technicians perform hands-on examination and diagnostics of network equipment on a routine and prescribed basis. Appendix F contains the SOW for Annual Preventive Maintenance.

1.1.5 Network Hardware Repair

Motorola provides a hardware repair service for all of the Motorola and select third-party infrastructure equipment supplied by Motorola. The Motorola authorized Repair Depot manages and performs the repair of Motorola supplied equipment as well as coordinating the equipment repair logistics process. Appendix C contains the SOW for Network Hardware Repair.

Network Hardware Repair with Advanced Replacement is a purchasable option under which Motorola will provide Customer with an advanced replacement unit(s) or Field Replacement Units (FRU's) as they are available in exchange for Customer's malfunctioning equipment. Malfunctioning equipment will be evaluated and repaired by the infrastructure repair depot and returned to depot's FRU inventory upon completion of repair. Customers who prefer to maintain their existing FRU inventory have an option to request a "Loaner" FRU while their unit is being repaired. If purchased, an appendix with the Network Hardware Repair with Advanced Replacement SOW will be included at the end of this document.

1.1.6 Security Management Operations

Remote Security Patch Installation

Motorola maintains a dedicated vetting lab for each supported ASTRO 25 release for the purpose of pre-testing security updates. In some cases, when appropriate, Motorola will make the updates available to outside vendors, allow them to test, and then incorporate those results into this offering. Once tested, Motorola posts the updates to a secured extranet website and sends an email notification to the customer. If there are any recommended configuration changes, warnings, or workarounds, Motorola will provide detailed documentation along with the updates on the website. In addition to testing the security updates, Remote Security Patch Installation includes remote installation of the updates. Appendix D contains the SOW for Remote Security Patch Installation.

Security Monitoring

ASTRO 25 Security Monitoring is a purchasable solution that provides 24x7x365 monitoring of the radio network security elements by specialized security technologists with years of experience working with ASTRO 25 mission-critical networks. For highly complex or unusual security events, our technologists have direct and immediate access to Motorola engineers for rapid resolution. If purchased, an appendix with the Security Monitoring SOW will be included at the end of this document.

1.1.7 MyView Portal

MyView Portal is a web-based platform that provides a transparent, single source view of network maintenance and operations along with historical system and service delivery information. It can be accessed from a desktop, laptop or tablet web browser.

- Event Monitoring Reports: See resolution status for incidents and notifications by Priority level.
- Technical Support: View Incident status details to compare them to committed response times.

- OnSite Support: Observe Incident details by Priority level and track the progress of onsite support issue resolution.
- Annual Preventive Maintenance: Access the maintenance status for all sites and quickly identify actions needed to take to optimize system performance. MyView Portal also allows downloading of blank checklists and upload of completed forms.
- Network Hardware Repair: Track return material authorizations (RMAs) shipped to our repair depot and eliminate the need to call for status updates.
- Security Patching: Receive automated patch downloads and status on competed updates.
- Trending Reports: Access up to 13 months of historical data and system activity to analyze Incident management.
- Asset and Contract Information: View all the assets purchased for the network, recent orders, and contract information.

The data presented in MyView Portal is in support of the appendix SOW's which provide the terms of any service delivery commitments associated with this data.

1.2 APPENDIX A: NETWORK EVENT MONITORING STATEMENT OF WORK

Network Event Monitoring provides real-time fault monitoring for radio communications networks on a continuous basis. Network Event Monitoring utilizes sophisticated tools for remote monitoring and event characterization of your communications networks. When an event is detected, skilled technologists acknowledge and assess the situation, and initiate a defined response.

The terms and conditions of this Statement of Work (SOW) are an integral part of Motorola's Service Agreement or other applicable agreement to which it is attached and made a part thereof by this reference.

1.0 Description of Network Event Monitoring Services

Network Event Monitoring is a service designed to monitor elements of a communication system for events, as set forth in the Monitored Elements Table. When the SSC detects an event, then, based on the Priority of the event, trained technologists acknowledge and remotely diagnose the event and initiate an appropriate response in accordance with the customer handling procedure. Appropriate responses could include, but are not limited to, continuing to monitor the event for further development, attempting remote remediation via engagement of Technical Support resources, or initiating dispatch of a Field Servicer ("Servicer") for onsite remediation if required.

1.1 Availability

Network Event Monitoring is available 24 hours a day, 7 days a week. Network Event Monitoring availability is based on the level of contracted service and defined in the Customer Support Plan (CSP).

1.2 Geographic Availability

Network Event Monitoring is a globally provided service unless limited by data export control regulations. Timeframes are based on the customer's local time zone.

1.3 Inclusions

Network Event Monitoring can be delivered on Motorola sold infrastructure as stated in the Monitored Elements Table.

1.4 Limitations and Exclusions

1.4.1 Does not include monitoring of anything outside of the radio network or monitoring of infrastructure provided by a third party, unless specifically stated. Monitored elements must be within the radio network and capable of sending traps to the Unified Event Manager (UEM).

1.4.2 Additional support charges above and beyond the contracted service agreement fees may apply if Motorola determines that system faults were caused by the customer making changes to critical system parameters.

1.4.3 The following activities are outside the scope of the Network Monitoring service, but are optional services that are available to remote Network Monitoring customers at an additional cost:

1.4.3.1 Emergency on-site visits required to resolve technical issues that cannot be resolved by SSC working remotely with the local customer technical resource.

1.4.3.2 System installations, upgrades, and expansions.

1.4.3.3 Customer training.

1.4.3.4 Hardware repair and/or exchange.

1.4.3.5 Network security services.

1.4.3.6 Network transport (WAN ports, WAN cloud, redundant paths).

1.4.3.7 Information Assurance.

1.4.3.8 Any services not expressly included in this statement of work.

1.4.4 Reference the event catalogue to confirm monitored equipment.

1.5 Motorola has the following responsibilities:

1.5.1. Provide dedicated connectivity through a network connection necessary for monitoring communication networks. The Connectivity Matrix further describes the connectivity options.

1.5.2 If determined necessary by Motorola, provide Motorola owned equipment for monitoring system elements. If Motorola installs or replaces Motorola owned equipment, the type of equipment and location installed is listed in the Motorola Owned & Supplied Equipment Table.

1.5.3 Verify connectivity and event monitoring prior to system acceptance or start date.

1.5.4 Monitor system continuously during hours designated in the CSP in accordance with the pre-defined times specified in section 1.6.2 below.

1.5.5 Remotely access the customer's system to perform remote diagnosis as permitted by customer pursuant to section 1.6.4.

1.5.6 Create a Incident, as necessary. Gather information to perform the following:

1.5.6.1 Characterize the issue

1.5.6.2 Determine a plan of action

1.5.6.3 Assign and track the Incident to resolution.

1.5.7 Cooperate with customer to coordinate transition of monitoring responsibilities between Motorola and customer as specified in section 1.6.13 and 1.6.13.1.

1.5.8 Maintain communication as needed with the customer in the field until resolution of the Incident

1.6 The Customer has the following responsibilities:

1.6.2 Allow Motorola continuous remote access to enable the monitoring service.

1.6.3 Provide continuous utility service to any Motorola equipment installed or utilized at customer's premises to support delivery of the service. Customer acknowledges Risk of loss to any Equipment provided to Customer as part of the Services will reside with Customer upon delivery and will remain with Customer until Equipment is returned to Motorola or its authorized representative.

1.6.4 Provide Motorola with pre-defined customer information and preferences prior to Start Date necessary to complete the CSP, including, but not limited to:

1.6.4.1 Incident notification preferences and procedure

1.6.4.2 Repair Verification Preference and procedure

1.6.4.3 Database and escalation procedure forms.

1.6.4.4 Submit changes in any information supplied to Motorola and included in the CSP to the CSM.

1.6.5 Provide the following information when initiating a service request:

1.6.5.1 Assigned system ID number

1.6.5.2 Problem description and site location

1.6.5.3 Other pertinent information requested by Motorola to open an Incident.

1.6.6 Notify the SSC when 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, or taking down part of the system to perform maintenance.)

1.6.7 Allow Servicers access to equipment (including any connectivity or monitoring equipment) if remote service is not possible.

1.6.8 Allow Servicers access to remove Motorola owned monitoring equipment upon cancellation of service.

1.6.9 Provide all customer managed passwords required to access the customer's system to Motorola upon request or when opening an Incident to request service support or enable response to a technical issue.

1.6.10 Pay additional support charges above and beyond 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

1.6.11 Obtain at Customer's cost all third party consents or licenses required to enable Motorola to provide the monitoring service.

1.6.12 Cooperate with Motorola and perform all acts that are reasonable or necessary to enable Motorola to provide the services described in this SOW.

1.6.13 Contact Motorola to coordinate transition of monitoring when monitoring responsibility is to be transferred to or from Motorola. (I.e. normal business hours to after-hours monitoring) as set forth in pre-defined information provided by customer CSP.

1.6.13.1.1 Upon contact, customer must provide customer name, site id, status on any open Incidents, Priority level, and brief description of Incident and action plan to Motorola.

1.6.14 Acknowledge that Incidents will be handled in accordance with the times and priorities as defined in the Event Definition table- Appendix A .

1.6.15 Cooperate with Motorola and perform all acts that are reasonable or necessary to enable Motorola to provide the Network Event Monitoring.

1.2.1 Engagement Matrix

The event types are based on the defined levels as follows:

Incident Priority	Definition	Engagement Times
Critical	**Core:** Core server failures Core Link failure **Sites/Subsites:** Entire Simulcast Not Wide Trunking >= 33% of Sites/subsites down	Response provided 24 hours, 7 days a week, including US Holidays.
High	- **Consoles:** Console positions down (>= 33%) Console Site Link Down - **Sites/Subsites:** < 33% of Sites/subsites down >= 33% of channels down - **Conventional Channels:** >= 50% of conventional channels (CCGW) down - **Devices:** Site Router/switch, GPS server down	Response provided 24 hours, 7 days a week, including US Holidays.
Medium	**Consoles:** Console positions down (< 33% at a site) **Sites/Subsites**: < 33% of channels down **Conventional Channels:** - Less than 50% of conventional channel down	Response provided 8 x 5 on standard business days, hours which is normally Monday through Friday 8AM to 5PM, excluding US Holidays.
Low	**Minor events and warnings in the system** - Preventative & Planned Maintenance Activities (Scheduled Work)	Response provided 8 x 5 on standard business days, which is normally Monday through Friday 8AM to 5PM, excluding US Holidays.

1.2.2 Connectivity Matrix

Request connectivity 8 weeks in advance of service start date.

System Type	Available Connectivity	Set up and Maintenance
ASTRO® 25	Internet VPN	Motorola
ASTRO® 25	Ethernet	Motorola

Motorola Owned & Supplied Equipment Table.

Equipment Type	Location Installed
Firewall/Router	Master Site
Service Delivery Management Server	Master Site for each Zone

Monitored Elements Table		
Switch	ATR	DNS
Firewall	AUC	Domain Controller
Gateway	Backup Server	Enrichment Testing
Router	Call Processor	Environmental
Virtual Machine	CAM	ESX
Network Device	Camera	EXINDA
Server	CCGW	Exit Router
Controller	Conventional	Gateway Unit
Base Radio	Core	Generic Node
Telephony	Core Router	Guest WIFI
Zone Controller	CPG	HSS
ADSP	Data Base station	IDF
Agent	Data Processing	Impact
AMB	Database Server	Infrastructure (CHI CAM)
AP	Device Config Server	Install Server
ARCA DACS	DIU	IPDU
Jump Server	Packet Data Gateway	WebGUI
LAN Switch	Moscad Server	Probe
Licensing Service	Net cool Server	Probe Server
Link	Network Address	PTT
Logging Recorder	NX	QUANTAR
Logging Replay Station	Object Server	RDM
LTE	OMADM	RFS
MDF	OP	RNG

Monitored Elements Table		
MGEG	OSP	RTU
Microwave	OSS	Security
MME	ZDS	Short Data Router
SPM	Statistical Server	TRAK
UPS	TENSR	Trap Forwarder
VMS	UEM	UCS
VPM	WebGUI	

*Some or all of the above equipment may be monitored depending on system configuration and need. Other equipment (not listed) may be monitored as an option, consult with your Customer Support Manager for details.

1.3 APPENDIX B: TECHNICAL SUPPORT STATEMENT OF WORK

Motorola's 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 Solutions Support Center (SSC) 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, reflecting the importance of maintaining mission critical systems.

1.1 Description of Technical Support Services

Motorola's Solutions Support Center's (SSC) primary goal is Customer Issue Resolution (CIR), providing Incident Restoration and Service Request Fulfillment on Motorola's currently supported infrastructure. This team of highly skilled, knowledgeable, and experienced specialists is available to the customer as an integrated part of the support and technical issue resolution process. The SSC remotely supports the customer and works with but not limited to fault diagnostics tools, simulation networks and fault database search engines.

Technical Support is available Monday - Friday 8:00am - 5:00pm local site time and 24 hours a day, 7 days a week for Critical, High Incidents. Technical Support availability for medium and low incidents is outlined in the Priority Level Response Goals. Calls requiring incidents or service requests will be logged in Motorola's Customer Relationship Management (CRM) system. This helps ensure that technical issues are prioritized, updated, tracked and escalated as necessary, until resolution. Technical Support Operations assigns the impact level in accordance with the agreed Priority Level Definitions stated in this document.

Motorola will track the progress of each Incident from initial capture to resolution. Motorola will advise and inform the customer of the Incident progress and tasks that require further investigation and assistance from the customer's technical resources.

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.

1.2 Scope

Technical Support service is available Monday - Friday 8:00am - 5:00pm local site time and 24 hours a day, 7 days a week for Critical and High Priority Incidents. See Priority Level Definitions.

1.3 Inclusions

Technical Support service will be delivered on Motorola sold infrastructure including integrated 3rd party products.

1.4 Limitations and Exclusions

The following activities are outside the scope of the Technical Support service, but are optional services that are available to remote Technical Support customers at an additional cost:

1.4.1 Emergency on-site visits required to resolve technical issues that cannot be resolved with the SSC working remotely with the local customer technical resource.

1.4.2 Third party support for equipment not sold by Motorola.

1.4.3 System installations, upgrades, and expansions.

1.4.4 Customer training.

1.4.5 Hardware repair and/or exchange.

1.4.6 Network security services.

1.4.7 Network transport management.

1.4.8 Motorola services not included in this statement of work.

1.4.9 Any technical support required as a result of a virus or unwanted intrusion is excluded if the system is not protected against these security threats by Motorola's Pre-tested Security Update Service when applicable.

1.5 Motorola has the following responsibilities:

1.5.1. Provide availability to the Motorola Solution Support Center (800-221-7144), 24 hours a day, 7 days a week to respond to Customer's requests for Critical and High priority Incidents support. Refer to Priority Level Response Time Goals for medium and low priority incident response times.

1.5.2. Respond initially to Incidents and Technical Service Requests in accordance with the response times set forth in the Priority Level Response Time Goals section of this document and the Priority level defined in the Priority Level Definitions section of this document.

1.5.3. Provide caller a plan of action outlining additional requirements, activities or information required to achieve restoral/fulfillment.

1.5.4. Maintain communication with the customer in the field as needed until resolution of the Incident

1.5.5. Coordinate technical resolutions with agreed upon third party vendors, as needed.

1.5.6. Manage functionally escalated support issues to additional Motorola technical resources, as applicable.

1.5.7. Determine, in its sole discretion, when a Incident requires more than the Technical Support services described in this SOW and notify customer of an alternative course of action.

1.6. The Customer has the following responsibilities:

1.6.1. Provide Motorola with pre-defined information prior to contract start date necessary to complete Customer Support Plan (CSP).

1.6.2. Submit changes in any information supplied in the Customer Support Plan (CSP) to the Customer Support Manager (CSM).

1.6.3. Contact the SSC in order to engage the Technical Support service, providing the necessary information for proper entitlement services. Including but not limited to the name of contact, name of customer, system ID number, site(s) in question, and brief description of the problem including pertinent information for initial issue characterization.

1.6.4. Maintain suitable trained technical resources that provide field maintenance and technical maintenance services to the system, and who are familiar with the operation of that system.

1.6.5. Supply suitably skilled and trained on-site presence when requested by the SSC.

1.6.6. Validate issue resolution prior to close of the Incident in a timely manner.

1.6.7. Acknowledge that Incidents will be handled in accordance with the times and priorities as defined in the Priority Level Definitions and in the Priority Level Response Time Goals section in this document.

1.6.8. Cooperate with Motorola and perform all acts that are reasonable or necessary to enable Motorola to provide the Technical Support

1.6.9 Obtain at Customer's cost all third party consents or licenses required to enable Motorola to provide the Service.

1.7 Technical Support Priority Level Definitions

The following Priority level definitions will be used to determine the maximum response times:

Incident Priority	Definition
Critical	**Core:** Core server failures Core Link failure **Sites/Subsites:** Entire Simulcast Not Wide Trunking >= 33% of Sites/subsites down
High	- **Consoles:** Console positions down (>= 33%) Console Site Link Down - **Sites/Subsites:** < 33% of Sites/subsites down >= 33% of channels down - **Conventional Channels:** >= 50% of conventional channels (CCGW) down - **Devices:** Site Router/switch, GPS server down
Medium	**Consoles:** Console positions down (< 33% at a site) **Sites/Subsites**: < 33% of channels down **Conventional Channels:** - Less than 50% of conventional channel down
Low	**Minor events and warnings in the system** - Preventative & Planned Maintenance Activities (Scheduled Work)

1.8 Technical Support Priority Level Response Goals

The response times are based on the defined Priority levels as follows:

Incident Priority	Response Time
Critical	A Motorola SSC Technician will make contact with the customer technical representative within one hour of the request for support being logged in the issue management system. Continual effort will be maintained to restore the system or provide a workaround resolution. Response provided 24 x 7.
High	A Motorola SSC Technician will make contact with the customer technical representative within four hours of the request for support being logged in the issue management system. Continual effort will be maintained to restore the system or provide a workaround resolution. Response provided 24 x 7.
Medium	A Motorola SSC Technician will make contact with the customer technical representative within four hours of the request for support being logged at the issue management system. Response provided 8 x 5 on standard business days, hours which is normally Monday through Friday 8AM to 5PM, excluding US Holidays.
Low	A Motorola SSC Technician will make contact with the customer technical representative within next business day of the request for support being logged at the issue management system. Response provided 8 x 5 on standard business days, which is normally Monday through Friday 8AM to 5PM, excluding US Holidays.

1.4 APPENDIX C: NETWORK HARDWARE REPAIR STATEMENT OF WORK

Motorola provides a hardware repair service for all of the Motorola and select third-party infrastructure equipment supplied by Motorola. The Motorola authorized Repair Depot manages and performs the repair of Motorola supplied equipment as well as coordinating the equipment repair logistics process.

1.1 Description of Services

Infrastructure components are repaired at a 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.

1.2 Scope

Repair Authorizations are obtained by contacting the Solutions Support Center (SSC) which is available 24 hours a day, 7 days a week.

Repair authorizations can also be obtained online via Motorola Online at https://businessonline.motorolasolutions.com, under Repair Status/Submit Infrastructure RA.

1.3 Inclusions

Network Hardware Repair is available on Motorola sold communication systems which may include some aspect of third party hardware and software. Motorola will make a "commercially reasonable effort" to repair Motorola manufactured infrastructure products for seven years after product cancellation.

1.4 Exclusions

If infrastructure is no longer supported by Motorola, the original equipment manufacturer or a third party vendor, Motorola may return said equipment to the customer without repair or replacement. The following items are excluded from Network Hardware Repair:

1.4.1 All Motorola infrastructure hardware over seven (7) years from product cancellation date.

1.4.2. All Third party infrastructure hardware over two (2) years from product cancellation date.

1.4.3. All Broadband infrastructure over three (3) years from product cancellation date

1.4.4. Physically damaged infrastructure.

1.4.5. Third party equipment not shipped by Motorola

1.4.6 Consumable items including, but not limited to, batteries, connectors, cables, toner/ink cartridges, tower lighting, laptop computers, monitors, keyboards and mouse.

1.4.7 Video retrieval from Digital In-Car Video equipment.

1.4.8 Infrastructure backhaul such as, Antennas, Antenna Dehydrator, Microwave[1], Line Boosters, Amplifier, Data Talker Wireless Transmitter, Short haul modems, UPS[1]

1.4.9 Test equipment.

1.4.10. Racks, furniture and cabinets.

1.4.11. Firmware and/or software upgrades.

[1] Excluded from service agreements but may be repaired on an above contract, time and material basis. All UPS Systems must be shipped to IDO for repair. Note! Excludes batteries and on-site services

1.5 Motorola has the following responsibilities:

1.5.1 Enable Customer access to the Motorola call Center operational 24 hours a day, 7 days per week, to create requests for repair service.

1.5.2 Provide repair return authorization numbers when requested by Customer.

1.5.3 Receive malfunctioning infrastructure from Customer and document its arrival, repair and return.

1.5.4 Perform the following service on Motorola infrastructure:

1.5.4.1 Perform an operational check on the infrastructure to determine the nature of the problem.

1.5.4.2. Replace malfunctioning Field Replacement Units (FRU) or components.

1.5.4.3. Verify that Motorola infrastructure is returned to Motorola manufactured specifications, as applicable.

1.5.4.4 Perform a box unit test on all serviced infrastructure.

1.5.4.5 Perform a system test on select infrastructure.

1.5.5 Provide the following service on select third party infrastructure:

1.5.5.1 Perform pre-diagnostic and repair services to confirm infrastructure malfunction and eliminate sending infrastructure with no trouble found (NTF) to third party vendor for repair, when applicable.

1.5.5.2 Ship malfunctioning infrastructure components to the original equipment manufacturer or third party vendor for repair service, when applicable.

1.5.5.3 Track infrastructure sent to the original equipment manufacturer or third party vendor for service.

1.5.5.4 Perform a post-test after repair by Motorola, original equipment manufacturer, or third party vendor to confirm malfunctioning infrastructure has been repaired and functions properly in a Motorola system configuration, when applicable.

1.5.5.5 Re-program repaired infrastructure to original operating parameters based on software/firmware provided by customer as required by section 1.6.7. If the customer software version/configuration is not provided, shipping times will be delayed. If the Infrastructure repair depot determines that the malfunctioning infrastructure is due to a software defect, the repair depot reserves the right to reload infrastructure with a similar software version.

1.5.5.6 Properly package repaired infrastructure.

1.5.5.7 Ship repaired infrastructure to the customer specified address during normal operating hours of Monday through Friday 7:00am to 7:00pm CST, excluding holidays. FRU will be sent two-day air unless otherwise requested. Motorola will pay for such shipping, unless customer requests shipments outside of the above mentioned standard business hours and/or carrier programs, such as NFO (next flight out). In such cases, customer will be responsible for payment of shipping and handling charges.

1.6 The Customer has the following responsibilities:

1.6.1 Contact or instruct Servicer to contact the Motorola Solutions Support Center (SSC) and request a return authorization number prior to shipping malfunctioning infrastructure.

1.6.2 Provide model description, model number and serial number, type of system, software and firmware version, symptom of problem and address of site location for FRU or infrastructure.

1.6.3 Indicate if infrastructure or third party infrastructure being sent in for service was subjected to physical damage or lightning damage.

1.6.4 Follow Motorola instructions regarding inclusion or removal of firmware and software applications from infrastructure being sent in for service.

1.6.5 Provide customer purchase order number to secure payment for any costs described herein.

1.6.6 Properly package and ship the malfunctioning FRU, at customer's expense. Customer is responsible for properly packaging the malfunctioning infrastructure FRU to ensure that the shipped infrastructure arrives un-damaged and in repairable condition.

1.6.6.1 Clearly print the return authorization number on the outside of the packaging.

1.6.7 Maintain versions and configurations for software/applications and firmware to install repaired equipment.

1.6.8 Provide Motorola with proper software/firmware information to reprogram equipment after repair unless current software has caused this malfunction.

1.6.9 Cooperate with Motorola and perform all acts that are reasonable or necessary to enable Motorola to provide the infrastructure repair services to customer.

1.6.10 Obtain at Customer's cost all third party consents or licenses required to enable Motorola to provide the Service.

1.5 APPENDIX D: REMOTE SECURITY PATCH INSTALLATION STATEMENT OF WORK

To verify compatibility with your ASTRO 25 system, Motorola's Remote Security Patch Installation provides pre-tested 3rd party software (SW) security updates.

In addition to testing the security updates, Remote Security Patch Installation includes remote installation of the updates.

This Statement of Work ("SOW") is subject to the terms and conditions of Motorola's Professional Services Agreement, Service Agreement or other applicable agreement in effect between the parties ("Agreement"). Motorola and Customer may be referred to herein individually as a "Party or together as "Parties"

1.1 Description of Remote Security Patch Installation

Motorola shall maintain a dedicated vetting lab for each supported ASTRO 25 release for the purpose of pre-testing security updates. In some cases, when appropriate, Motorola will make the updates available to outside vendors, allow them to test, and then incorporate those results into this offering. Depending on the specific ASTRO 25 release and customer options, these may include updates to antivirus definitions, OEM vendor supported Windows Workstation and Server operating system patches, Solaris and Red Hat Linux (RHEL) operating system patches, VMware ESXi Hypervisor patches, Oracle database patches, PostgreSQL patches, and patches for other 3rd party Windows applications such as Adobe Acrobat and Flash.

Motorola has no control over the schedule of releases. The schedule for the releases of updates is determined by the Original Equipment Manufacturers (OEMs), without consultation with Motorola. Antivirus definitions are released every week. Microsoft patches are released on a monthly basis. Motorola obtains and tests these updates as they are released. Other products have different schedules or are released "as-required." Motorola will obtain and test this OEM vendor supported updates on a quarterly basis.

1.2 Connectivity

To accommodate remote installation of security updates, a connection is required from Motorola to the customer ASTRO 25 network. There are two different options. 1) T1 line purchased and maintained by Motorola, or 2) The customer internet connection is used and a Virtual Private Network (VPN) is established between Motorola and the ASTRO 25 network. Since this relies on the customer internet connection, the customer is responsible for the availability of the connection.

Along with the connection itself, Motorola supplied hardware is required to be deployed to the customer premises on the ASTRO 25 network. Motorola shall load software, configure, and ship the hardware to the customer supplied contact for installation. This hardware and its maintenance is part of the connectivity service.

ASTRO 25 connectivity is ordered separately from Remote Security Patch Installation and has a separate statement of work. See that SOW for more detail on terms of the connection.

If connectivity is already established for a different service such as network or security monitoring then the same connection can be used for Remote Security Patch Installation. There is no need for a separate connection to be established.

1.3 Security Update Installation

Motorola shall push the tested security updates over the established connection. The timing and coordination with the customer of each update depends on the updates themselves. Motorola requires IP connectivity to all elements that are in scope for patching. If IP connectivity from Motorola is not available then those elements will not be considered for remote patching and will require alternative arrangements outside of the scope of this statement of work.

1.3.1 Antimalware Signature Update Installation

Antimalware signature updates are released often, but Motorola collects and tests them on a weekly basis. The updates are non-intrusive (for example, no reboots or manual configuration changes are required) and automatically implemented. Therefore, antimalware signature updates will be pushed within a week of testing without Customer coordination. An email will be sent to inform the Customer that the signatures have been updated.

1.3.2 Microsoft Windows Security Update Installation

Microsoft typically releases security updates every second Tuesday of the month (aka “Patch Tuesday”); however, selected security updates are sometimes released on other days, and it is possible that no security updates are released during a month. Security updates for some 3rd party Windows software (Non-Motorola and non-Microsoft applications that run on Windows, such as Adobe Reader and Flash) are also released on Patch Tuesday. The most recent Windows and 3rd party Windows security updates available will be acquired by Motorola on each Patch Tuesday. These patch security updates require at least one week for incorporation into the offering and a minimum of 36 hours for testing in the Motorola vetting labs, after which security updates with no issues are then released. Patches may be held back at the discretion of Motorola if they are found to cause any problems to features, performance or functionality and will only be released when the issues are fully resolved.

It is important to understand that it is often the case that after security updates are installed, Microsoft requires the patched computer to be rebooted before the security updates take full effect and vulnerabilities are mitigated. The clients include dispatch consoles and there is no way for Motorola to know when it is safe to reboot. The customer must reboot at a time chosen by them so as to not impact operations.

Once the security updates are vetted, Motorola will start pushing the updates to the customer without customer coordination or notification. An email will be sent requesting that the clients be rebooted. It is the customer’s responsibility to reboot all of the clients before the next set update is sent. When preparing for the next month’s push of security updates, Motorola will first scan to verify all of the previous updates were implemented and if any computer has not been rebooted. Motorola will send an email requesting that the remaining computers be rebooted before any new updates are pushed.

1.3.3 Microsoft Windows Security Updates Outside ASTRO 25 Firewalls

Connections to other networks (from now on referred to as Customer Enterprise Network, or CEN) must be delineated by firewalls. All updates deployed by Remote Security Patch Installation are specific to equipment inside the ASTRO 25 Radio Network with only the following exceptions: Key Management Facility (KMF), Text messaging Services (TMS) and advanced Messaging Services (AMS) and MCC 7100 consoles. In these exceptions, the customer has a choice of including these machines in the Remote Security Patch Installation service, or including them in their own IT security patch procedures.

The KMF, TMS, and AMS are all outside the firewall (relative to the Radio Network) and therefore updates require that the firewall be opened. The default for Remote Remote Security Patch Installation is that these functions are included.

The MCC 7100 console may be directly on the radio network or in the CEN. Any MCC 7100 on the radio network would simply be included in the standard Remote Security Patch Installation offering. However, the MCC 7100 may also be located in the CEN and connected through a VPN to a firewall at a dispatch location. In this case, the default for Remote Security Patch Installation is to not update these consoles.

If the customer requires inclusion for the CEN based MCC 7100 consoles, then they must contact their Customer Service Manager and make a formal request. They must also consent to allow Motorola to open the firewall to allow access for updates.

1.3.4 Quarterly Security Update Installation

The quarterly patch updates are for Solaris and Red Hat Linux (RHEL) operating systems, and VMWare ESXi hypervisor (virtualization). They are tested and released on a quarterly basis, at end of March, June, September, and December. Motorola will schedule installation of the updates with the customer in the first weeks of the following quarter. Motorola will send the customer an ITIL with details on the upgrade and scheduling for each of the events.

These updates are intrusive and require customer coordination. Examples of how they affect the customer include reboots to implement the patches and rolling (switching from one zone controller to the other) of the zone controllers. Systems with redundant zone controllers (L2, M2, M3) have low downtime (minutes) as the zone controllers are rolled, but systems with single zone controllers (L1, M1) will be down for longer periods. During these times, the system will be in “Site trunking” mode. It is up to the customer to understand the operational impacts and to coordinate these events with users.

This effort will be done during standard business hours, or 8am to 5pm CST. Customers requesting that downtime be during non-standard hours must submit an official request through their CSM. The ITIL will show work being done during standard hours such as prep work, downloading of the patches to memory, etc and the actual reboots or ZC rollover will be initiated when requested. Additional remote work will proceed the next day during standard hours.

Motorola System Enhancement Releases (“SERs”) and Field Service Bulletins (“FSB’s) are not part of this service. However in some instances, these fixes must be done to allow the latest security patches. If it is possible for the specific required FSB to be installed remotely, then Motorola will include it as part of Remote Security Patch Installation. Otherwise, Motorola will communicate this to the customer and the patches that cannot be delivered.

The Customer and their CSM will determine how to get the SER or FSB installed. Once the SER or FSB appears on the system, Remote Security Patch Installation will then install the affected patches.

For minimal downtime and to avoid redundant efforts, the customer should coordinate any maintenance or other updates such as FSB's and SER's with Motorola.

1.4 Scope

Remote Security Patch Installation supports the currently shipping Motorola ASTRO 25 System Release (SR) and strives to support five (5) releases prior. Motorola reserves the right to adjust which releases are supported as business conditions dictate. Contact your Customer Service Manager for the latest supported releases.

Remote Security Patch Installation is available for any L or M core system in a supported release. Remote Security Patch Installation is not available for K cores.

Systems that have non-standard configurations that have not been certified by Motorola Systems Integration and Testing (SIT) are specifically excluded from this Service unless otherwise agreed in writing by Motorola. Service does not include pre-tested intrusion detection system (IDS) updates for IDS solutions. Certain consoles, MOTOBRIDGE, MARVLIS, Symbol Equipment, AirDefense Equipment, AVL, Genesis, WAVE and Radio Site Security products are also excluded. Motorola will determine, in its sole discretion, the third party software that is supported as a part of this offering.

1.5 Motorola has the following responsibilities:

1.5.1 Obtain relevant third party software ("SW") security updates as made available from the OEM's. This includes antivirus definition updates, operating systems patches, hypervisor patches, database patches, and selected other third party patches that Motorola deployed in ASTRO 25 system releases covered by this Remote Security Patch Installation. Motorola does not control when these updates are released, but as much as possible vet the updates on this schedule:

McAfee Antivirus definitions– Weekly

Windows OS updates – Monthly

Solaris, RHEL OS, VMware ESXi updates – Quarterly

1.5.2 Each assessment of relevant third party SW will take at least one week to incorporate the security updates into the Remote Security Patch service and 36 additional hours of examination time to evaluate the impact each update has on the system.

1.5.3 Perform rigorous testing of updates to verify whether they degrade or compromise system functionality on a dedicated ASTRO 25 test system with standard supported configurations.

1.5.4 Address any issues identified during testing by working as necessary with Motorola selected commercial supplier(s) and/or Motorola product development engineering

team(s). If a solution for the identified issues cannot be found, the patch will not be posted on Motorola's site.

1.5.5 Pre-test STIG recommended remediation when applicable.

1.5.6 Release all tested updates to Motorola's secure extranet site.

1.5.7 Coordinate updates with customer as outlined in section 1.

1.5.8 In the event that no updates are released by the OEM's during the usual time period, Motorola will send a notice that no new patches were sent.

1.5.9 Notify customer of update releases by email.

1.5.10 A supported Remote Security Patch Installation ASTRO 25 release matrix will be kept on the extranet site for reference.

1.6 The Customer has the following responsibilities:

1.6.1 This service requires connectivity from Motorola to the customer's ASTRO 25 system. This connectivity must be established prior to service start.

1.6.2 Maintain IP connectivity from Motorola to all elements in the system that require remote patching.

1.6.3 Provide Motorola with pre-defined information (customer contacts, system information, etc) prior to contract start date necessary to complete a Customer Support Plan (CSP).

1.6.4 Submit changes in any information supplied in the Customer Support Plan (CSP) to the Customer Support Manager (CSM).

1.6.5 Upgrade system to a supported system release as necessary to continue service.

1.6.6 Refrain from making uncertified changes of any type to the system.

1.6.7 Adhere closely to the System Support Center (SSC) troubleshooting guidelines provided upon system acquisition. A failure to follow SSC guidelines may cause the customer and Motorola unnecessary or overly burdensome remediation efforts. In such case, Motorola reserves the right to charge an additional service fee for the remediation effort.

1.6.8 Comply with the terms of the applicable software license agreement(s) between the Customer and Motorola and non-Motorola software copyright owner.

1.6.9. Obtain at Customer's cost all third party consents or licenses required to enable Motorola to provide the Service.

1.6.10 Upon successful installation of patches on windows clients (e.g. Dispatch Ops Position, NM Client, etc.) and receiving notification indicating the task has been successfully executed by Motorola, affected computers must be rebooted by the customer within 72 hours.

1.6.11 Understand downtime implications associated with reboots and patch activities and internally coordinate with users as necessary.

1.7 Disclaimer:

Motorola disclaims any and all warranties with respect to pre-tested antivirus definitions, database security updates, hypervisor patches, operating system software patches, intrusion detection sensor signature files, or other 3rd party files, express or implied. Further, Motorola disclaims any warranty concerning the non-Motorola software and does not guarantee that customer's system will be error-free or immune to security breaches as a result of these services.

1.6 APPENDIX E: ONSITE SUPPORT STATEMENT OF WORK

Motorola's OnSite Support service provides Incident management and escalation for onsite technical service requests. The service is delivered by the Motorola's Solutions Support Center (SSC) in conjunction with a local service provider. The SSC is responsible for opening an Incident for onsite support and monitoring the status of that Incident to maintain response time conformance.

The terms and conditions of this Statement of Work (SOW) are an integral part of Motorola's Service Agreement or other applicable agreement to which it is attached and made a part thereof by this reference.

Description of Services

The Motorola SSC will receive customer request for OnSite service provider and dispatch a servicer. The servicer will respond to the customer location based on pre-defined Priority Levels set forth in Priority Level Definitions table and Response times set forth in Priority Level Response Time Goals table in order to restore the system.

Motorola will provide Incident management as set forth herein. The SSC will maintain contact with the on-site Motorola Service Shop until system restoral and Incident closure. The SSC will continuously track and manage Incidents from creation to close through an automated Incident tracking process.

1.1 Scope

OnSite Support is available 24 hours a day, 7 days a week in accordance with Priority Level Definitions and Priority Level Response Time Goals tables.

1.2 Inclusions

Onsite Support can be delivered on Motorola-sold infrastructure.

2.0 Motorola has the following responsibilities:

2.1. Receive service requests.

2.2. Create an Incident as necessary when service requests are received. Gather information to characterize the issue, determine a plan of action and assign and track the Incident to resolution.

2.3. Dispatch a field servicer ("Servicer") as required by Motorola's standard procedures and provide necessary Incident information.

2.4. Provide the required personnel access to relevant customer information as needed.

2.5. Servicer will perform the following on-site:

2.6. Run diagnostics on the Infrastructure or Field Replacement Units (FRU).

2.7. Replace defective Infrastructure or FRU, as supplied by customer.

2.8. Provide materials, tools, documentation, physical planning manuals, diagnostic/test equipment and any other requirements necessary to perform the maintenance service.

2.9. If a third party vendor is needed to restore the system, the Servicer may accompany that vendor onto the customer's premises.

2.10. Verify with customer that restoration is complete or system is functional, if required by customer's repair verification in the Customer Support Plan. If verification by customer cannot be completed within 20 minutes of restoration, the Incident will be closed and the Servicer will be released.

211. Escalate the Incident to the appropriate party upon expiration of a response time.

2.12. Close the Incident upon receiving notification from customer or servicer, indicating the Incident is resolved.

2.13. Notify customer of Incident status as defined by the Customer Support Plan:

2.13.1 Open and closed; or

2.13.2 Open, assigned to the servicer, arrival of the servicer on-site, deferred or delayed, closed.

2.14. Provide Incident activity reports to customer if requested.

3.0 Customer has the following responsibilities:

3.1. Contact Motorola, as necessary, to request service.

3.2. Provide Motorola with the following pre-defined customer information and preferences prior to start date necessary to complete Customer Support Plan (CSP):

3.2.1. Incident notification preferences and procedure.

3.2.2. Repair verification preference and procedure.

3.2.3. Database and escalation procedure forms.

3.2.4. Submit changes in any information supplied in the CSP to the Customer Support Manager (CSM).

3.3. Provide the following information when initiating a service request:

3.3.1. Assigned system ID number.

3.3.2. Problem description and site location.

3.3.3. Other pertinent information requested by Motorola to open a Incident.

3.4. Allow Servicers access to equipment.

3.5. Supply infrastructure or FRU, as applicable, in order for Motorola to restore the system.

3.6. Maintain and store in an easily accessible location any and all software needed to restore the system.

3.7. Maintain and store in an easily accessible location proper system backups.

3.8 For E911 systems, test the secondary/backup Public Safety Answering Point (PSAP) connection to be prepared in the event of a catastrophic failure of a system. Train appropriate personnel on the procedures to perform the function of switching to the backup PSAP.

3.9 Verify with the SSC that restoration is complete or system is functional, if required by repair verification preference provided by customer.

3.10. Cooperate with Motorola and perform all acts that are reasonable or necessary to enable Motorola to provide these services.

3.11. Obtain and provide applicable third party consents or licenses at Customer cost to enable Motorola to provide the Services.

4.0 Onsite support Priority Level Definitions

The following Priority level definitions will be used to determine the maximum response times:

Incident Priority	Definition
Critical	**Core:** Core server failures Core Link failure **Sites/Subsites:** Entire Simulcast Not Wide Trunking >= 33% of Sites/subsites down
High	- **Consoles:** Console positions down (>= 33%) Console Site Link Down - **Sites/Subsites:** < 33% of Sites/subsites down >= 33% of channels down - **Conventional Channels:** >= 50% of conventional channels (CCGW) down - **Devices:** Site Router/switch, GPS server down
Medium	**Consoles:** Console positions down (< 33% at a site) **Sites/Subsites**: < 33% of channels down **Conventional Channels:** - Less than 50% of conventional channel down
Low	**Minor events and warnings in the system** - Preventative & Planned Maintenance Activities (Scheduled Work)

5.0 Priority Level Response Time Goals

(Customer's Response Time Classification is designated in the Customer Support Plan.)

Incident Priority Level	Standard Response Time
Critical	Within 4 hours from receipt of notification continuously
High	Within 4 hours from receipt of notification continuously
Medium	Within 8 hours from receipt of notification Standard Business Day, Hours(8-5pm local time)
Low	Within 12 hours from receipt of notification Standard Business Day, Hours(8-5pm local time)

* Premier Response is an option that can be purchased, it provides a 2-hour response time for Critical /High Priority Incidents (as applicable)

1.7 APPENDIX F: ANNUAL PREVENTIVE MAINTENANCE STATEMENT OF WORK

The terms and conditions of this Statement of Work (SOW) are an integral part of Motorola's Service Agreement or other applicable agreement to which it is attached and made a part thereof by this reference.

Annual Preventative Maintenance will provide annual operational tests on the customer's infrastructure equipment (Infrastructure or Fixed Network Equipment or "FNE") to monitor the Infrastructure's conformance to specifications, as set forth in the applicable attached Exhibit(s), all of which are hereby incorporated by this reference.

1.1 Scope

Annual Preventive Maintenance will be performed during standard business hours (unless otherwise agreed to in writing). If the system or Customer requirements dictate this service must occur outside of standard business hours, an additional quotation will be provided. Customer is responsible for any charges associated with unusual access requirements or expenses.

1.2 Inclusions

Annual Preventive Maintenance service will be delivered on Motorola sold infrastructure including integrated 3rd party products per the level of service as defined in Table 1.

1.3 Limitations and Exclusions

Unless specifically called out in Table 1, the following activities are outside the scope of the Annual Preventive Maintenance service, however, can be included as optional services that are available to Annual Preventive Maintenance customers at an additional cost:

1.3.1. Emergency on-site visits required to resolve technical issues.

1.3.2. Third party support for equipment not sold by Motorola as part of the original system.

1.3.3. System installations, upgrades, and expansions.

1.3.4. Customer training.

1.3.5. Hardware repair and/or exchange.

1.3.6. Network security services.

1.3.7. Transport link performance verification.

1.3.8. Information Assurance.

1.3.9. Motorola services not included in this statement of work.

1.3.10. Any maintenance required as a result of a virus or unwanted intrusion is excluded if the system is not protected against these security threats by Motorola's Pre-tested Security Update Service when applicable.

1.3.11. Tower climbs, tower mapping analysis or tower structure analysis

1.4 Motorola has the following responsibilities:

1.4.1. Notify the customer of any planned system downtime needed to perform this Service.

1.4.2. Advise customer of issues that may require attention.

1.4.3. Maintain communication with the customer as needed until completion of the Annual Preventive Maintenance.

1.4.4. Determine, in its sole discretion, when a Incident requires more than the Annual Preventive Maintenance services described in this SOW and notify customer of an alternative course of action.

1.4.5. Provide customer with a report documenting system performance against expected parameters along with recommended actions. Time allotment for report completion TBD.

1.4.6. Provide trained and qualified personnel with proper security clearance required to complete Annual Preventive Maintenance services.

1.5 The Customer has the following responsibilities:

1.5.1. Provide preferred schedule for Annual Preventative Maintenance to Motorola.

1.5.2. Authorize and acknowledge any scheduled system downtime.

1.5.3. Maintain periodic backup of databases, software applications, and firmware.

1.5.4. Establish and maintain a suitable environment (heat, light, and power) for the equipment location 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.

1.5.5. Submit changes in any information supplied in the Customer Support Plan (CSP) to the Customer Support Manager (CSM).

1.5.6. Provide site escorts in a timely manner if required.

1.5.7. Provide Motorola with requirements necessary for access to secure facilities.

1.5.8. Obtain at Customer's cost all third party consents or licenses required to enable Motorola to provide the Service

1.6 The Servicer has the following responsibilities:

1.6.1.Perform the Preventive Maintenance tasks as set forth in Table 1 at the level of service the customer has purchased.

1.6.2.Perform the Site Performance Verification Procedures in Table 2 for each site type on the system.

1.6.3. Provide required diagnostic/test equipment necessary to perform the Preventive Maintenance service.

As applicable, use the Method of Procedure (MOPs) as defined for each task.

MASTER 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.
NM Client Applications	Review UEM events and transport medium types, (microwave/leased line/telco, etc). Event log review for persistent types. Verify all NM client applications are operating correctly.
Verify System SW CD's	Perform audit of software media on site. Versions, KC numbers, types, etc.
Complete Backup	Verify backups have been done or scheduled. SZ database (BAR), Centracom CDM/ADM database, etc.
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 are up to date (within two weeks of current date) on CSMS
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 CWR devices. Core router switchover (coordinate 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 CWR devices. Core router switchover (coordinate with customer).
DOMAIN CONTROLLERS (non-CSA)	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.

MASTER SITE CHECKLIST - LEVEL 1	
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Verify System SW CD's	Perform audit of software media on site. Versions, KC numbers, types, etc.
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	I.e. memory, HDD, CPU, disk space/utilization.

PRIME SITE CHECKLIST - LEVEL 1	
SOFTWARE	
Verify System SW CD's	Perform audit of software media on site. Versions, KC numbers, types, etc.
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 antistatic vacuum to clean cooling pathways
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 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.

PRIME SITE CHECKLIST - LEVEL 1	
Site Frequency Standard Check (TRAK)	Check lights and indicators for A/B receivers.
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 antistatic vacuum to clean cooling pathways
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 antistatic vacuum to clean cooling pathways

DISPATCH SITE CHECKLIST - LEVEL 1	
GENERAL	
Inspect all Cables	Inspect all cables/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 Op Time	Verify console op time is consistent across all ops
Screensaver	Verify screensaver set as customer prefers
Screen Performance	Verify screen operational/performance
Touchscreen	Verify touch screen operation (if applicable)
Cabling/Lights/Fans	Visual inspection of all equipment - cabling/ lights/ fans
Filters/Fans/Dust	Clean any filters/ fans/ dust- all equipment
Monitor and Hard Drive	Confirm monitor and hard drive do not "sleep"
DVD/CD	Verify / 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 are up to date (within two weeks of current date)
HEADSET UNPLUGGED TESTING	
Speakers	Test all speakers - audio quality, volume, static, drop-outs, excess hiss when turned up.

DISPATCH SITE CHECKLIST - LEVEL 1	
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 select speaker muted.
Telephone Operation	Verify telephone operational through both headset jacks. Check volume controls for noise/static or drop-outs.
Audio Switches	Verify select audio switches to speaker when phone off-hook. (if interfaced to phones)
Radio Takeover in Headset	Verify radio-takeover in headset mic when phone off-hook (mic switches to radio during PTT and mutes to phone).
OTHER TESTS	
Phone Status Light	Verify phone status light comes on when phone off-hook (if applicable)
Desk Microphone Operation	Confirm desk mic operation (if applicable)
Radio IRR Operation	Verify radio IRR operational (if applicable) on MOT dispatch
Telephone IRR Operation	Verify telephone [if on radio computer] IRR operational (if applicable) on MOT dispatch
Recording	Verify operator position being recorded on long term logging recorder (if applicable) if included in service agreement
COMPUTER PERFORMANCE TESTING	
Computer Reboot	Reboot op position computer
Computer Operational	Confirm 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 op position
Backup Resources	Confirm backup resources are operational
EQUIPMENT ROOM TESTS	

DISPATCH SITE CHECKLIST - LEVEL 1	
Recording - AIS Test	Verify audio logging of trunked calls
Recording	Test op position logging on analog recorder (with customer assistance)
System Alarms	Review alarm system on all equipment for errors
Capture Diagnostics	Perform recommended diagnostic tests based on equipment. Capture available diagnostic logs.
Verify System SW CD's	Perform audit of software media on site. Versions, KC numbers, types, etc.
PLAYBACK STATION (Motorola Provided)	
Capture Diagnostics	Perform recommended diagnostic tests based on equipment. Capture available diagnostic logs.
Recall Audio	Verify that radio/telephone audio can be recalled

RF SITE CHECKLIST - LEVEL 1	
RF PM CHECKLIST	
Equipment Alarms	Verify no warning/alarm indicators.
Clean Fans and Equipment	Use antistatic vacuum to clean cooling pathways
Site Frequency Standard Check	Check lights and indicators for A/B receivers.
Basic Voice Call Check	Voice tests each voice path, radio to radio.
Control Channel Redundancy (trunking)	Roll control channel, test, and roll back.
Site Controller Redundancy (trunking) - ASR only	Roll site controllers with no dropped audio.
PM Optimization Workbook	Complete RF Site PM Checks - Frequency Error, Modulation Fidelity, Forward at Set Power, Reverse at Set Power, Gen Level Desense no Tx

MOSCAD CHECKLIST - LEVEL 1	
MOSCAD SERVER	
Equipment Alarms	Verify no warning/alarm 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	Site devices to verify passwords. Document changes if any found.

MOSCAD CHECKLIST - LEVEL 1	
Verify System SW CD's	Perform audit of software media on site. Versions, KC numbers, types, etc.
MOSCAD CLIENT	
Equipment Alarms	Verify no warning/alarm 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	Site devices to verify passwords. Document changes if any found.
Verify System SW CD's	Perform audit of software media on site. Versions, KC numbers, types, etc.
MOSCAD RTU's	
Equipment Alarms	Verify no warning/alarm indicators.
Verify Connectivity	Verify Connectivity
Password Verification	Site devices to verify passwords. Document changes if any found.
Check Alarm/Event History	Review MOSCAD alarms and events to find if there are chronic issues.
Verify System SW CD's	Perform audit of software media on site. Versions, KC numbers, types, etc.

FACILITIES CHECKLIST - LEVEL 1	
VISUAL INSPECTION EXTERIOR	
ASR Sign	Verify that the ASR sign is posted.
Warning Sign - Tower	Verify 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/photocell.
Exterior of Building	Check exterior of building for damage/disrepair.
Fences / Gates	Check fences/gates for damage/disrepair.
Landscape / Access Road	Check landscape/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.

FACILITIES CHECKLIST - LEVEL 1	
Equipment Inspection	Visually inspect that all hardware (equipment, cables, panels, batteries, racks, etc.) are in acceptable physical condition for normal operation.
Regulatory Compliance (License, ERP, Frequency, Deviation)	Check station for regulatory compliance. Update station logs.
Clean Fans and Equipment	Use antistatic vacuum to clean cooling pathways
UPS	
Visual inspection (condition, cabling)	Verify corrosion, physical connections, dirt/dust, etc.
GENERATOR	
Visual Inspection	Verify, check panel housing, cracks, rust and weathering. Physical connections, corrosion, dirt/dust, etc.
Fuel	Verify fuel levels in backup generators, document date of last fuel delivered from fuel service provider.
Oil	Check the oil dipstick for proper level. Note condition of oil.
Verify operation (no switchover)	Check, verify running of generator, ease of start or difficult. Is generator "throttling" or running smooth? Any loud unusual noise? Etc.
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 outdoor unit is unobstructed
Wiring	Wiring (insect/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.
RADIO	
Alarms	Check alarm / event history
Software	Verify version of application
TX Frequency	Verify transmit frequency

MICROWAVE CHECKLIST - LEVEL 1	
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
Backhaul Performance	Monitor UEM status (alarms, logs, etc.) for all links. If UEM not used to monitor microwave, then use provided microwave alarm mgmt server.
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 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 (NO TOWER CLIMB)	
STRUCTURE CONDITION(From ground level only)	
Rust	Check structure for rust.
Cross Members	Check for damaged or missing cross members.
Safety Climb	Check safety climb for damage.
Ladder	Verify that ladder system is secured to 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 paint condition.
TOWER LIGHTING	
Lights/Markers	Verify all lights/markers are operational.
Day/Night Mode	Verify day and night mode operation.
Power Cabling	Verify that power cables are secured to 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.

TOWER CHECKLIST - LEVEL 1 (NO TOWER CLIMB)	
GROUNDING	
Structure Grounds	Inspect grounding for damage or corrosion
GUY WIRES	
Tower Guys	Check guy wires for fraying and tension.
Guy Wire Hardware	Check hardware for rust.
CONCRETE CONDITION	
Tower Base	Check for chips or cracks.

SECTION 2

LIFECYCLE STATEMENT OF WORK

The following SUA II Statement of Work fully describes the SUA II offering.

2.1 ASTRO 25 SYSTEM UPGRADE AGREEMENT II (SUA II)

1.0. Description of Service and Obligations

1.1. As system releases become available, Motorola agrees to provide the Customer with the software, hardware and implementation services required to execute up to one system infrastructure upgrade in a two-year period for their ASTRO 25 system. At the time of the system release upgrade, Motorola will provide applicable patches and service pack updates when and if available. Currently, Motorola's service includes 3rd party SW such as Microsoft Windows and Server OS, Red Hat Linux, Sun Solaris and any Motorola software service packs that may be available. Motorola will only provide patch releases that have been analyzed, pre-tested, and certified in a dedicated ASTRO 25 test lab to ensure that they are compatible and do not interfere with the ASTRO 25 network functionality. Additionally, if purchased, the Security Update Service (SUS) coverage is defined in Appendix C.

1.2. The Customer will have, at its option, the choice of upgrading in either Year 1 or Year 2 of the coverage period. To be eligible for the ASTRO 25 SUA II, the ASTRO 25 system must be at system release 7.7 or later.

1.3. ASTRO 25 system releases are intended to improve the system functionality and operation from previous releases and may include some minor feature enhancements. At Motorola's option, system releases may also include significant new feature enhancements that Motorola

may offer for purchase. System release software and hardware shall be pre-tested and certified in Motorola's Systems Integration Test lab.

1.4. The price quoted for the SUAII requires the Customer to choose a certified system upgrade path from the list of System Release Upgrade Paths available to the Customer as per the system release upgrade chart referenced and incorporated in Appendix A. Should the Customer elect an upgrade path other than one listed in Appendix A, the Customer agrees that additional costs may be incurred to complete the implementation of the certified system upgrade. In this case, Motorola agrees to provide a price quotation for any additional materials and services necessary.

1.5. ASTRO 25 SUA II entitles a Customer to past software versions for the purpose of downgrading product software to a compatible release version.

1.6. The following ASTRO 25 certified system release software for the following products are covered under this ASTRO 25 SUA II: base stations, site controllers, comparators, routers, LAN switches, servers, dispatch consoles, logging equipment, network management terminals, Network Fault Management ("NFM") products, network security devices such as firewalls and intrusion detection sensors, and associated peripheral infrastructure software.

1.7. Product programming software such as Radio Service Software ("RSS"), Configuration Service Software ("CSS"), and Customer Programming Software ("CPS") are also covered under this SUA II.

1.8. ASTRO 25 SUA II makes available the subscriber radio software releases that are shipping from the factory during the SUA II coverage period. New subscriber radio options and features not previously purchased by the Customer are excluded from ASTRO 25 SUA II coverage. Additionally, subscriber software installation and reprogramming are excluded from the ASTRO 25 SUA II coverage.

1.9. Motorola will provide certified hardware version updates and/or replacements necessary to upgrade the system with an equivalent level of functionality up to once in a two-year period. Hardware will be upgraded and/or replaced if required to maintain the existing feature and functionality. Any updates to hardware versions and/or replacement hardware required to support new features or those not specifically required to maintain existing functionality are not included. Unless otherwise stated, platform migrations such as, but not limited to, stations, consoles, backhaul, civil, network changes and additions, and managed services are not included.

1.10. The following hardware components, if originally provided by Motorola, are eligible for full product replacement when necessary per the system release upgrade:

1.10.1. Servers

1.10.2. PC Workstations

1.10.3. Routers

1.10.4. LAN Switches

1.11. The following hardware components, if originally provided by Motorola, are eligible for board-level replacement when necessary per the system release upgrade. A "board-level replacement" is defined as any Field Replaceable Unit ("FRU") for the products listed below:

1.11.1. GTR 8000 Base Stations

1.11.2. GCP 8000 Site Controllers

1.11.3. GCM 8000 Comparators

1.11.4. MCC 7XXX Console Operator Positions

1.11.5. STR 3000 Base Stations

1.11.6. Quantar Base Stations

1.11.7. Centracom Gold Elite Console Operator Interface Electronics

1.11.8. Centracom Gold Elite Central Electronics Banks

1.11.9. Ambassador Electronics Banks

1.11.10. Motorola Gold Elite Gateways

1.11.11. ASTROTAC Comparators

1.11.12. PSC 9600 Site Controllers

1.11.13. PBX Switches for Telephone Interconnect

1.11.14. NFM/NFM XC/MOSCAD RTU

1.12. The ASTRO 25 SUA II does not cover all products. Refer to section 3.0 for exclusions and limitations.

1.13. Motorola will provide implementation services necessary to upgrade the system to a future system release with an equivalent level of functionality up to once in a two-year period. Any implementation services that are not directly required to support the certified system upgrade are not included. Unless otherwise stated, implementation services necessary for system expansions, platform migrations, and/or new features or functionality that are implemented concurrent with the certified system upgrade are not included.

1.14. As system releases become available, Motorola will provide up to once in a two-year period the following software design and technical resources necessary to complete system release upgrades:

1.14.1. Review infrastructure system audit data as needed.

1.14.2. Identify additional system equipment needed to implement a system release, if applicable.

1.14.3. Complete a proposal defining the system release, equipment requirements, installation plan, and impact to system users.

1.14.4. Advise Customer of probable impact to system users during the actual field upgrade implementation.

1.14.5. Program management support required to perform the certified system upgrade.

1.14.6. Field installation labor required to perform the certified system upgrade.

1.14.7. Upgrade operations engineering labor required to perform the certified system upgrade.

1.15. ASTRO 25 SUA II pricing is based on the system configuration outlined in Appendix B. This configuration is to be reviewed annually from the contract effective date. Any change in system configuration may require an ASTRO 25 SUA II price adjustment.

1.16. The ASTRO 25 SUA II applies only to system release upgrades within the ASTRO 25 7.x platform.

1.17. Motorola will issue Software Maintenance Agreement ("SMA") bulletins on an annual basis and post them in soft copy on a designated extranet site for Customer access. Standard and optional features for a given ASTRO 25 system release are listed in the SMA bulletin.

2.0. Upgrade Elements and Corresponding Party Responsibilities

2.1. Upgrade Planning and Preparation: All items listed in this section are to be completed at least 6 months prior to a scheduled upgrade.

2.1.1. Motorola Responsibilities

2.1.1.1. Obtain and review infrastructure system audit data as needed.

2.1.1.2. Identify additional system equipment needed to implement a system release, if applicable.

2.1.1.3. Complete a proposal defining the system release, equipment requirements, installation plan, and impact to system users.

2.1.1.4. Advise Customer of probable impact to system users during the actual field upgrade implementation.

2.1.1.5. Inform Customer of high speed internet connection requirements.

2.1.1.6. Assign program management support required to perform the certified system upgrade.

2.1.1.7. Assign field installation labor required to perform the certified system upgrade.

2.1.1.8. Assign upgrade operations engineering labor required to perform the certified system upgrade.

2.1.1.9. Deliver release impact and change management training to the primary zone core owners, outlining the changes to their system as a result of the upgrade path elected. This training needs to be completed at least 12 weeks prior to the scheduled upgrade. This training will not be provided separately for user agencies who reside on a zone core owned by another entity. Unless specifically stated in this document, Motorola will provide this training only once per system.

2.1.2. Customer responsibilities

2.1.2.1. Contact Motorola to schedule and engage the appropriate Motorola resources for a system release upgrade.

2.1.2.2. Provide high-speed internet connectivity at the zone core site(s) for use by Motorola to perform remote upgrades and diagnostics. Specifications for the high-speed connection are provided in Appendix D. High-speed internet connectivity must

be provided at least 12 weeks prior to the scheduled upgrade. In the event access to a high-speed connection is unavailable, Customer may be billed additional costs to execute the system release upgrade.

2.1.2.3. Assist in site walks of the system during the system audit when necessary.

2.1.2.4. Provide a list of any FRUs and/or spare hardware to be included in the system release upgrade when applicable.

2.1.2.5. Purchase any additional software and hardware necessary to implement optional system release features or system expansions.

2.1.2.6. Provide or purchase labor to implement optional system release features or system expansions.

2.1.2.7. Participate in release impact training at least 12 weeks prior to the scheduled upgrade. This applies only to primary zone core owners. It is the zone core owner's responsibility to contact and include any user agencies that need to be trained or to act as a training agency for those users not included.

2.2. System Readiness Checkpoint: All items listed in this section must be completed at least 30 days prior to a scheduled upgrade.

2.2.1. Motorola responsibilities

2.2.1.1. Perform appropriate system backups.

2.2.1.2. Work with the Customer to validate that all system maintenance is current.

2.2.1.3. Work with the Customer to validate that all available patches and antivirus updates have been updated on the customer's system.

2.2.2. Customer responsibilities

2.2.2.1. Validate system maintenance is current.

2.2.2.2. Validate that all available patches and antivirus updates to their system have been completed.

2.3. System Upgrade

2.3.1. Motorola responsibilities

2.3.1.1. Perform system infrastructure upgrade in accordance with the system elements outline in this SOW.

2.3.2. Customer responsibilities

2.3.2.1. Inform system users of software upgrade plans and scheduled system downtime.

2.3.2.2. Cooperate with Motorola and perform all acts that are reasonable or necessary to enable Motorola to provide software upgrade services.

2.4. Upgrade Completion

2.4.1. Motorola responsibilities

2.4.1.1. Validate all certified system upgrade deliverables are complete as contractually required.

2.4.1.2. Deliver post upgrade implementation training to the customer as needed, up to once per system.

2.4.1.3. Obtain upgrade completion sign off from the customer.

2.4.2. Customer Responsibilities

2.4.2.1. Cooperate with Motorola in efforts to complete any post upgrade punch list items as needed.

2.4.2.2. Cooperate with Motorola to provide relevant post upgrade implementation training as needed. This applies only to primary zone core owners. It is the zone core owner's responsibility to contact and include any user agencies that need to be trained or to act as a training agency for those users not included.

2.4.2.3. Provide Motorola with upgrade completion sign off.

3.0. Exclusions and Limitations

3.1. The parties agree that Systems that have non-standard configurations that have not been certified by Motorola Systems Integration Testing are specifically excluded from the ASTRO 25 SUA II unless otherwise agreed in writing by Motorola and included in this SOW.

3.2. The parties acknowledge and agree that the ASTRO 25 SUA II does not cover the following products:

- MCC5500 Dispatch Consoles
- MIP5000 Dispatch Consoles
- Plant/E911 Systems
- MOTOBRIDGE Solutions
- ARC 4000 Systems
- Motorola Public Sector Applications Software ("PSA")
- Custom SW, CAD, Records Management Software
- Data Radio Devices
- Mobile computing devices such as Laptops
- Non-Motorola two-way radio subscriber products
- Genesis Products
- Point-to-point products such as microwave terminals and association multiplex equipment

3.3. ASTRO 25 SUA II does not cover any hardware or software supplied to the Customer when purchased directly from a third party, unless specifically included in this SOW.

3.4. ASTRO 25 SUA II does not cover software support for virus attacks or other applications that are not part of the ASTRO 25 system, or unauthorized modifications or other misuse of the covered software. Motorola is not responsible for management of anti-virus or other security applications (such as Norton).

3.5. Upgrades for equipment add-ons or expansions during the term of this ASTRO 25 SUA II are not included in the coverage of this SOW unless otherwise agreed to in writing by Motorola.

4.0. Special provisions

4.1. Customer acknowledges that if its System has a Special Product Feature, additional engineering may be required to prevent an installed system release from overwriting the Special Product Feature. Upon request, Motorola will determine whether a Special Product Feature can be incorporated into a system release and whether additional engineering effort is required. If additional engineering is required Motorola will issue a change order for the change in scope and associated increase in the price for the ASTRO 25 SUA II.

4.2. Customer will only use the software (including any System Releases) in accordance with the applicable Software License Agreement.

4.3. ASTRO 25 SUA II services do not include repair or replacement of hardware or software that is necessary due to defects that are not corrected by the system release, nor does it include repair or replacement of defects resulting from any nonstandard, improper use or conditions; or from unauthorized installation of software.

4.4. ASTRO 25 SUA II coverage and the parties' responsibilities described in this Statement of Work will automatically terminate if Motorola no longer supports the ASTRO 25 7.x software version in the Customer's system or discontinues the ASTRO 25 SUA II program; in either case, Motorola will refund to Customer any prepaid fees for ASTRO 25 SUA II services applicable to the terminated period.

4.5. If Customer cancels a scheduled upgrade within less than 12 weeks of the scheduled on site date, Motorola reserves the right to charge the Customer a cancellation fee equivalent to the cost of the pre- planning efforts completed by the Motorola Solutions Upgrade Operations Team.

4.6. The SUA II annualized price is based on the fulfillment of the two-year term. If Customer terminates, except if Motorola is the defaulting party, Customer will be required to pay for the balance of payments owed if a system release upgrade has been taken prior to the point of termination.

4.7. In additional to any terms set forth herein, Motorola's contract with the CSA signed by the parties on December 21, 2018, will apply to this SUA transaction. The System upgrade will be scheduled during the subscription period and will be performed when Motorola's system upgrade operation resources are available. Because there might be a significant period from when a System upgrade transaction is performed, Motorola may substitute any of the promised Equipment or Software so long as the substitute is equivalent or superior to the initially promised Equipment or Software.

4.8. Acceptance of a SUA transaction occurs when the Equipment (if any) and Software are delivered and the SUA services are fully performed; there is no Acceptance Testing with a SUA transaction. The Warranty Period for any Equipment or Motorola Software provided under a SUA transaction will commence upon shipment and not on System Acceptance or Beneficial Use, and is for a period of ninety (90) days rather than one (1) year.

4.9. In addition to the description of the SUA services and exclusions provided in the SUA Statement of Work, the following apply:

a) Upon reasonable request by Motorola, Customer will provide a complete serial and model number list of the Equipment.

b) SUA services exclude the repair or replacement of Equipment that has become defective or damaged from use in other than the normal, customary, intended, and authorized manner; use not in compliance with applicable industry standards; excessive wear and tear; or accident, liquids, power surges, neglect, acts of God or other force majeure events.

c) Unless specifically included herein, SUA services exclude items that are consumed in the normal operation of the Equipment; accessories; and repair or maintenance of any transmission line, antenna, microwave equipment, tower or tower lighting, duplexer, combiner, or multicoupler. Motorola has no obligations for any transmission medium, such as telephone lines, computer networks, the internet or the worldwide web, or for Equipment malfunction caused by the transmission medium.

d) Customer will provide Motorola with designated points of contact (list of names and phone numbers) that will be available during the performance of the SUA services.