



MOTOROLA SOLUTIONS

Proposal

City of Gahanna, Ohio

AXS Dispatch Console Project

March 13, 2025

The design, technical, and price information furnished with this proposal is proprietary information of Motorola Solutions, Inc. (Motorola). Such information is submitted with the restriction that it is to be used only for the evaluation of the proposal, and is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the proposal, without the express written permission of Motorola Solutions, Inc.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2025 Motorola Solutions, Inc. All rights reserved.

PS-000188700

Motorola Solutions, Inc.
500 W Monroe St
Chicago, IL 60661

March 13, 2025

Chief Spence
City of Gahanna Police Department
460 Rocky Fork Blvd
Gahanna, OH 43230

Subject: AXS Dispatch Console Conversion, Addition of (2) AXS Consoles and Archive Interface Server (AIS)

Dear Chief Spence,

Motorola Solutions, Inc. ("Motorola") is pleased to have the opportunity to provide City of Gahanna with a dispatch console move, upgrade and addition. The Motorola project team has taken great care to propose a solution to address your needs and provide exceptional value.

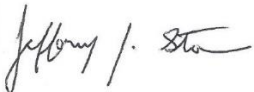
Motorola's solution includes a combination of hardware, software and services. Specifically, this solution provides:

- Move & Conversion of (5) existing MCC7500 operator positions to the AXS platform.
- Addition of (2) AXS operator positions.
- Addition of an Archive Interface Server (AIS).
- Implementation and warranty services.

This proposal is subject to the terms and conditions of the enclosed Motorola Solutions Customer Agreement (MCA) and remains valid until June 09, 2025. City of Gahanna may accept this proposal by signing and returning a copy of the MCA. Alternatively, Motorola would be pleased to address any concerns regarding this proposal. Any questions can be directed to Jaime Myers, Account Executive, at (937) 701-8931 or jaime.myers@motorolasolutions.com.

Our goal is to provide City of Gahanna with the best product and services available in the communications industry. We thank you for the opportunity, and we hope to strengthen our relationship by implementing this solution.

Sincerely,



Jeff Stowasser
MSSI Vice President
MOTOROLA SOLUTIONS, INC.

Table of Contents

Section 1

System Overview..... 1-1

1.1 Dispatch Console Overview..... 1-1

1.1.1 Integration with the ASTRO® 25 Network..... 1-1

1.1.2 Connection the ASTRO® 25 System 1-2

1.1.3 Dispatch Operator Positions..... 1-2

1.2 AXS Dispatch Console Solution 1-3

1.3 Making Consoles Easy to Operate 1-3

1.3.1 Next Generation Dispatch Experience 1-3

1.3.2 Cross Platform Dispatch Capabilities 1-5

1.3.3 Headset Sharing..... 1-5

1.3.4 Standard Radio Transmission and Reception..... 1-5

1.3.5 Emergency Radio Transmission and Reception 1-7

1.3.6 Radio Patch Control 1-7

1.3.7 Call Management and Control..... 1-8

1.3.8 Enhanced Integrated Instant Recall Recorder (IRR)..... 1-9

1.3.9 MKM 7000 Console Alias Manager (CAM) 1-9

1.4 Protecting Consoles and Communications 1-9

1.4.1 Secure Access to the Console 1-9

1.4.2 Secure Communications at the Console 1-9

1.5 Dispatch Console Solution Components..... 1-10

1.5.1 CommandCentral AXS Dispatch Console Operator Position 1-10

1.6 Conventional Channel Gateways 1-11

1.7 Spares 1-12

1.8 Logging Interface 1-12

1.9 Archiving Interface Server 1-12

1.9.1 Archiving Interface Server Equipment Overview..... 1-12

1.9.2 Archiving Interface Server Session Limitations..... 1-13

1.9.3 Archiving Interface Server Application Programming Interface (API) 1-13

1.9.4 Firewall 1-14

1.10 DSC 8000 Site Controller..... 1-14

1.11 MC Edge Aux I/O..... 1-14

1.12 Assumptions..... 1-14

Section 2

Equipment List..... 2-1

Section 3

Statement of Work..... 3-1

3.1	Overview	3-1
3.1.1	Motorola's Responsibilities	3-1
3.1.2	City of Gahanna Responsibilities	3-2
3.2	Project Schedule	3-5

Section 4

Warranty & Maintenance Plan	4-1
4.1 Warranty Support Services	4-1
4.2 ASTRO 25 Advanced Plus Services Statement of Work	4-1
4.2.1 Overview	4-1
4.3 Motorola Service Delivery Ecosystem	4-3
4.4 Centralized Managed Support Operations	4-3
4.5 Field Service	4-4
4.6 Customer Support Manager	4-4
4.7 Customer Hub	4-4
4.8 Connectivity Specifications	4-5
4.9 Advanced Plus Services Detailed Description	4-5
4.10 ASTRO System Monitoring (NEW)	4-5
4.10.1 Managed Detection and Response	4-5
4.10.1.1 Description of Service	4-6
4.10.1.2 Managed Detection and Response Elements	4-6
4.10.1.3 Deployment Timeline and Milestones	4-8
4.10.1.4 General Responsibilities	4-9
4.10.1.5 Service Modules	4-11
4.10.1.6 Network Detection	4-12
4.10.1.7 Endpoint Detection and Response	4-12
4.10.1.8 External Vulnerability Scanning	4-13
4.10.1.9 Security Operations Center Monitoring and Support	4-13
4.10.1.10 Incident Response	4-15
4.10.1.11 Event Response and Notification	4-15
4.10.1.12 Notification	4-16
4.10.1.13 Tuning	4-16
4.10.1.14 Tuning Period Exception	4-16
4.10.1.15 Incident Priority Level Definitions and Response Times	4-17
4.10.1.16 Included Services	4-18
4.10.1.17 Limitations and Exclusions	4-19
4.10.2 Network Event Monitoring	4-21
4.10.2.1 Description of Service	4-21
4.10.2.2 Scope	4-22
4.10.2.3 Inclusions	4-22
4.10.2.4 Connectivity	4-25
4.10.2.5 Motorola Owned and Supplied Equipment	4-26
4.10.2.6 Monitored Elements	4-26

4.10.3	ASTRO Connectivity Services.....	4-27
4.10.4	Remote Technical Support.....	4-29
4.10.4.1	Description of Service.....	4-29
4.10.4.2	Scope.....	4-29
4.10.4.3	Inclusions.....	4-30
4.10.5	Network Hardware Repair with Advanced Replacement	4-31
4.10.5.1	Description of Service.....	4-31
4.10.5.2	Scope.....	4-31
4.10.5.3	Inclusions.....	4-31
4.10.5.4	Repair Process	4-34
4.10.5.5	Advanced Replacement	4-35
4.10.5.6	Replacement Process for Advanced Replacement.....	4-37
4.10.6	Security Update Service	4-38
4.10.6.1	Description of Service.....	4-38
4.10.6.2	On-Site Delivery	4-39
4.10.6.3	Reboot Support	4-39
4.10.6.4	Scope.....	4-39
4.10.6.5	Inclusions.....	4-39
4.10.6.6	Installation and Reboot Responsibilities.....	4-41
4.10.7	Remote Security Update Service	4-42
4.10.7.1	Description of Service.....	4-42
4.10.7.2	Application of Prerequisite Motorola Technical Notices (MTN)	4-43
4.10.7.3	Updates to System Components in the Customer Enterprise Network	4-43
4.10.7.4	Microsoft Windows Reboot Following Security Update Installation	4-43
4.10.7.5	Reboot Support	4-44
4.10.7.6	Scope.....	4-44
4.10.7.7	Tenanted Customers Access to Antivirus Updates	4-45
4.10.7.8	Inclusions.....	4-45
4.10.7.9	Reboot Responsibilities	4-46
4.10.8	On-Site Infrastructure Response.....	4-47
4.10.8.1	Description of Service.....	4-48
4.10.8.2	Scope.....	4-48
4.10.8.3	Geographical Availability	4-48
4.10.8.4	Inclusions.....	4-48
4.10.8.5	Priority Level Definitions and Response Times.....	4-50
4.10.9	Annual Preventative Maintenance.....	4-52
4.10.9.1	Description of Service.....	4-52
4.10.9.2	Scope.....	4-53
4.10.9.3	Inclusions.....	4-53
4.10.9.4	Preventative Maintenance Tasks	4-54
4.10.10	System Upgrade Agreement (SUA)	4-61
4.10.10.1	Overview.....	4-61
4.10.10.2	Scope.....	4-62
4.10.10.3	Inclusions.....	4-62

4.10.10.4	System Upgrades	4-63
4.10.10.5	Subscriber Radio Software	4-63
4.10.10.6	Limitations and Exclusions	4-63
4.10.10.7	Platform Migrations.....	4-63
4.10.10.8	Non-Standard Configurations.....	4-64
4.10.10.9	System Expansions and New Features	4-64
4.10.10.10	Cloud Technology.....	4-64
4.10.10.11	Subscriber Radio Software	4-64
4.10.10.12	General Statement of Work for System Upgrades	4-64
4.10.10.13	System Readiness Checkpoint	4-66
4.10.10.14	System Upgrade.....	4-66
4.10.10.15	Upgrade Completion.....	4-66
4.10.10.16	Special Provisions	4-67
Appendix A: ASTRO 25 System Release Upgrade Paths		4-67
Appendix B: System Pricing Configuration		4-68
Appendix C: SUA Coverage Table		4-69
4.11	Priority Level Definitions and Response Time	4-71
4.12	Appendix 1 ASTRO 25 Remote Security Update Coverage	4-72
4.12.1	RSUS Coverage	4-72
4.13	Exclusions	4-74
Section 5		
Training Plan.....		5-1
5.1	Overview	5-1
5.2	Training Approach.....	5-1
5.3	Proposed Courses.....	5-2
5.4	Seven Position Training.....	5-2
5.4.1	Console Operator and Supervisor Training Plan	5-2
5.5	Course Outlines.....	5-3
5.5.1	AXS Operator	5-3
5.5.2	AXS Supervisor	5-4
Section 6		
Pricing Summary		6-1
6.1	AXS Dispatch Site	6-1
6.2	Pricing Terms and Conditions	6-1
6.3	Maintenance and Lifecycle Services	6-1
Section 7		
Contractual Documentation.....		7-1

Section 1

System Overview

1.1 Dispatch Console Overview

This proposal is for a Motorola AXS console dispatch system to support the operations of Gahanna PD. The console system will provide Gahanna PD with a new dispatch site consisting of (7) AXS platform console positions.

The new dispatch site will connect to the State of Ohio MARCS system (utilizing customer provided backhaul) and the back-room console dispatch site equipment will be utilized to support the customer provided logging recorder, and conventional radio resources, as applicable.

This proposal includes the addition of the following equipment at the Gahanna PD's dispatch site:

- (7) AXS Operator Positions
- (1) DSC 8000 Backup Site Controller
- (1) CAM
- (1) Auxiliary Input/Output Server
- (2) CCGW
- (1) Archiving Interface Server (AIS)
- (1) Firewall/CEN Switch
- (2) Switches
- (2) Routers

The proposed AXS console equipment connects directly to the trunking system's transport network. It uses IP-based packet protocols for passing call control data and call audio through the system.

NOTE: Gahanna PD is responsible for all connectivity, per Motorola specification, to the Ohio MARCS Core.

NOTE: It is assumed Gahanna PD's AXS console operator will utilize only certified AXS third party co-hab applications.

1.1.1 Integration with the ASTRO® 25 Network

The proposed dispatch console seamlessly integrates into the ASTRO® 25 system for an integrated, mission-critical network. This tight union between radio infrastructure and console equipment has several operational benefits to Gahanna PD's. The physical space to accommodate the proposed console is comparable to that required for a personal computer.

The console can access both trunked talkgroups and conventional radio channels over the same network. This architecture reduces overall transport costs and the need for duplicate fixed network equipment.

1.1.2 Connection the ASTRO® 25 System

The ASTRO 25 system's architecture is flexible and can be configured to meet Gahanna PD's unique needs. Gahanna PD is responsible for the connectivity of the new dispatch to the core.

Dual Site Link

The proposed console site for Gahanna PD's is remote from the core site and features redundant site links to provide path diversity. The console site has two logical connections to the core site, with each connection using a different core router.

Each console site gateway provides an interface that handles the following IP traffic between the proposed console center Gahanna PD's ASTRO 25 Core site:

- Network Management traffic.
- Call control and audio traffic for all the calls being handled by the dispatch positions.
- Aux I/O traffic for the Aux I/Os being handled by the dispatch positions.
- The site gateways fragment and prioritize large IP packets according to industry standards and convert Ethernet data to the desired transport medium.

Encrypted Site Link

The gateway encryption feature uses an AES 256-bit encryption algorithm for all voice and data packets between the console site and the core site. All packets traveling through these WAN links, which are provided by a public network service provider to Gahanna PD's, are encrypted.

LAN Switches

LAN switches provide LAN interfaces for console site equipment and a LAN port for the link to the core site. Service technicians can access the system's configuration manager and service the equipment through the switch.

1.1.3 Dispatch Operator Positions

The CommandCentral AXS dispatch console consists of the CommandCentral Hub running on a Windows Operating System, while the GUI is displayed on the Edgeweb browser.

Dispatch Console Hardware

The CommandCentral AXS dispatch console solution can be enhanced through dispatch peripherals, such as speakers, microphone, headset jack, and footswitch. These peripherals are designed for 24/7 usage without degradation in performance or reliability.

The CommandCentral AXS dispatch console equipment includes the following hardware elements per operator position:

- (7) CommandCentral Hub
- (7) Monitors
- (4) Speakers per Op
- (7) Microphones
- (2) Footswitches

- (2) Headsets/Headset jacks per Op

NOTE: Existing Headsets/ Headset jack boxes and footswitches will be provided by the customer from the existing (5) Gahanna operator positions at the MECC dispatch.

1.2 AXS Dispatch Console Solution

Motorola Solutions, Inc.'s (Motorola) CommandCentral AXS Dispatch Console reduces the barriers between systems in the Gahanna PD's dispatch center, allowing access to all the mission-critical tools and applications dispatchers need in the moments that matter. This makes operation more efficient in emergency situations. Resources are accessible with an intuitive, highly configurable browser-based GUI. Dispatchers will have an expansive feature set and a mission-critical IP network for transporting information and calls throughout the system.

CommandCentral AXS improves the efficiency and operation of dispatchers in the following ways. Additional fees may apply depending upon feature and hardware additions:

- **Next Generation Dispatch Experience** – The solution responds to touch, type, or click, giving dispatchers the flexibility to interact and stay connected to teams in the way that best suits them. Extensive configuration options, flexible deployment configurations, and simple scalability means agencies only pay for what is needed now, with the room to adapt and grow as needs change over time.
- **Purpose-Built Dispatch Console Accessories** – Enhances the dispatch experience with accessories, such as gooseneck microphone, speakers, headset jack, and footswitch, designed and tested for industry-leading performance and reliability.

The AXS solution also reduces operating costs and provides a smaller physical footprint in the command center without compromising on features or reliability. This combination of seamless communications, modern architecture, and advanced integration capabilities enables the CommandCentral AXS solution to scale and evolve as needs change over time.

1.3 Making Consoles Easy to Operate

Motorola's proposed consoles are optimized for real-time audio, prioritizing emergency calls over other traffic, and minimizing voice queuing. Using robust error mitigation to maintain call quality even when the system is heavily loaded, the proposed console reduces communication errors that may force dispatchers or radio users to repeat their transmissions.

1.3.1 Next Generation Dispatch Experience

CommandCentral AXS features a highly configurable graphical user interface (GUI) that provides quick, single-view access to important information and functionalities. The browser-based GUI's versatile folders, tabs, and scalable resources allow users to organize and configure their dispatch experience and make engagement more familiar and intuitive from shift to shift. Folders and tabs can be relocated, exposed, or overlapped as needed, giving dispatchers more control of what information, they see and how they interact with those resources. CommandCentral AXS also offers multiple options for routing audio to speakers and controlling volume levels.

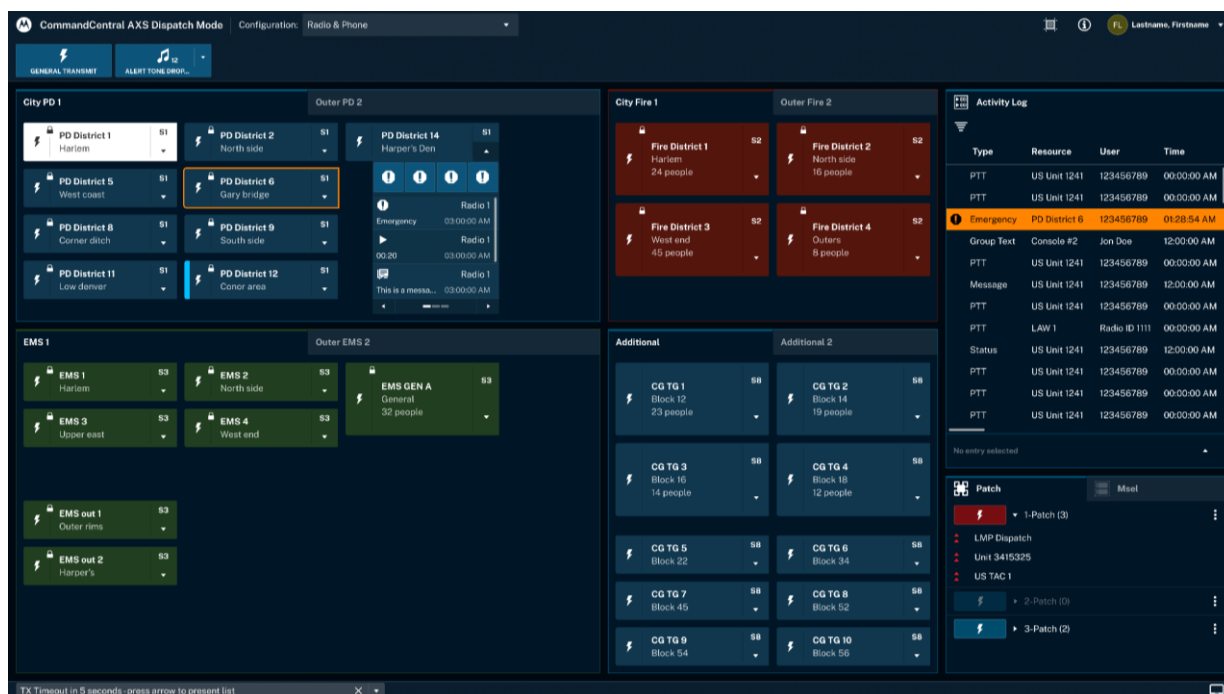


Figure 1-1: Next Generation Dispatch Experience

CommandCentral AXS features flexible window positioning and capabilities for quick and efficient access to services such as:

- **Activity Log** – Provides an efficient point of reference for all incoming calls into a dispatch console, showing dispatchers detailed, searchable call information (radio resource name and call time) to enable faster and more informed response.
- **Paging** – Allows users to send user configured pages on radio resources. This flexible paging feature is integrated with CommandCentral AXS for both conventional and trunked radio resources, while an external paging encoder port on the CommandCentral Hub enables third-party paging encoders to send pages on the selected radio resources.
- **Patch Capabilities** – Enables dispatchers to set up a communication path between two or more resources that are normally unable to communicate with each other, such as trunked resources and conventional resources.
- **Alert Tones** – Allows dispatchers to send one of fifteen user-configurable alert tones on selected radio resources. Fifteen default .wav files are provided with the dispatch console software, but any combination of these default files may be replaced with user configured .wav files to meet specific needs.
- **Channel Marker** – Enables dispatchers to send a periodically repeating piece of audio on radio resources to meet the specific needs.

1.3.2 Cross Platform Dispatch Capabilities

This solution is designed to take full advantage of Motorola's end-to-end software suite, CommandCentral. These cross-platform integrations enhance the dispatch capabilities of CommandCentral AXS.

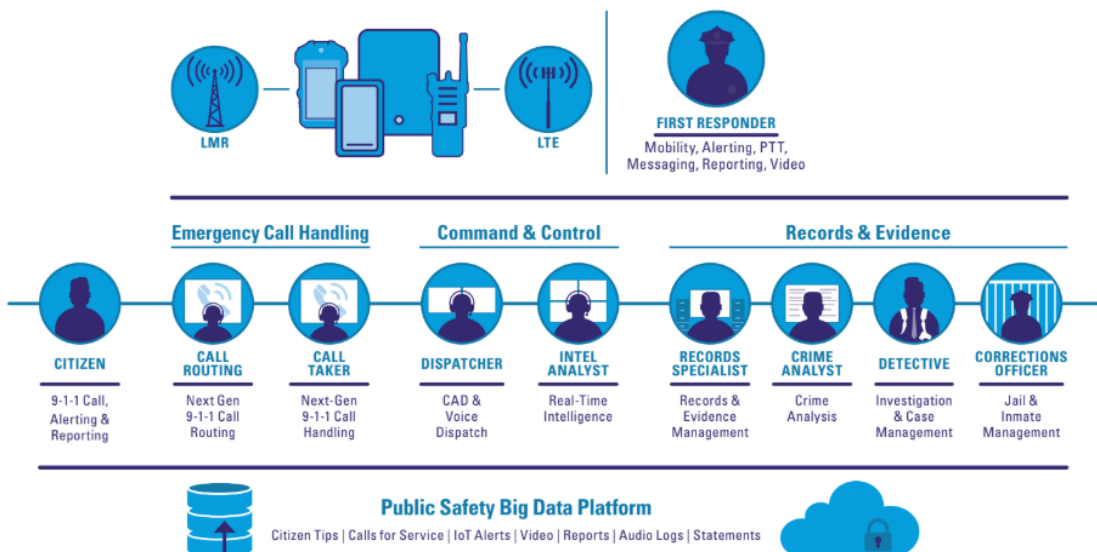


Figure 1-2: Motorola's End-to-End Portfolio

CommandCentral AXS is an integral part of our end-to-end portfolio, providing greater interoperability and support for Gahanna's PD current and future investments. As needs grow and change over time, this solution's flexible integration capabilities evolve to satisfy new demands. This adaptability also enables dispatchers to be effective with the integrations and capabilities they need.

1.3.3 Headset Sharing

CommandCentral AXS supports Headset Sharing, which enables a dispatcher to use a common headset for both radio and 911 communications and to quickly access basic 911 call taking functionality from CommandCentral AXS. This improves the dispatcher's efficiency and accuracy when they have to concentrate on the radio dispatch GUI while handling 911 calls.

1.3.4 Standard Radio Transmission and Reception

A typical proposed dispatch position has a headset and two speakers. One speaker is for selected audio and the second speaker is for all remaining unselected audio. Additional speakers can be added to a console allowing dispatchers to configure a specific speaker for a set of designated audio sources. This simplifies multitasking between multiple audio sources and allows flexibility in the way the audio is presented to the dispatcher.

Receiving Calls from the Field and Other Dispatchers

The proposed console provides dispatchers with greater flexibility for how to hear calls from field radio users and other dispatchers. Each dispatcher can define his or her own audio reception profile by selecting a single audio source, whether conventional or talkgroup, to be heard on a selected speaker or headset (Single Select). The dispatcher can also define groups of radio resources that can all be heard on a selected speaker or headset (Multi-Select).

Initiating Calls to the Field and Other Dispatchers

The dispatcher has several different ways of initiating a call. In most circumstances, a General Transmit is appropriate. With the General Transmit, the dispatcher selects a resource on the console and activates the transmission through a footswitch, headset transmit button, or a microphone transmit button. If the dispatcher needs to quickly transmit on a resource that is not selected, the dispatcher uses the Instant Transmit function.

A safety switch is available, which prevents accidental activation of functions that may cause negative consequences. The safety switch can be used with Aux I/Os and preprogrammed pages, as well as Instant Transmit switches.

Audio Communication to the Field and Other Dispatchers

The dispatcher can transmit audio in different ways. They can make calls to all users listening to a specific conventional radio resource or a specific trunking talkgroup. When multiple resources are required, the dispatcher can select additional talkgroups and/or conventional channels, as needed using the Multi-Select feature.

The proposed console also enables dispatchers to make private calls to individual field radio users or dispatchers. Once a private call is established, it can be patched in with another resource at the dispatcher's discretion.

Controlling Console Audio

The proposed console offers dispatchers several different ways of controlling or muting the audio on their consoles, such as the following:

- Audio volume can be changed for any specific resource.
- All non-selected resources on the console can be muted for 30 seconds (All Mute) or unmuted, if already muted.
- A dispatcher can transmit on a resource while receiving audio from the same resource or other resources.
- A dispatch position can be configured to automatically mute the other dispatch audio on a shared resource to prevent acoustic feedback when a co-located dispatch position transmits.
- RF Cross Mute automatically mutes the receive audio from a specified channel when the dispatcher transmits on another specified channel to prevent acoustic feedback.

Controlling Network Audio

Dispatchers can control audio on the ASTRO® 25 network. The dispatcher can enable or disable radio users to compartmentalize traffic, reduce interruptions, and maintain communications between dispatch and the field. When this function is enabled or disabled, all dispatch consoles with this resource assigned are updated with the current status of the feature. This feature can be controlled from any dispatch position.

1.3.5 Emergency Radio Transmission and Reception

As part of a mission-critical communications network, the proposed dispatch console facilitates immediate prioritization and resolution of emergency communications between dispatch and first responders in the field. This enables dispatchers and first responders to focus on their mission and not their equipment, especially during critical situations.

Receiving an Emergency Call

When a user in the field or another dispatcher initiates an emergency call, the console emits both visual and audible indications (Emergency Alarm). The audible indication alerts the dispatcher that an emergency is underway; the visual indication directs the dispatcher's attention to the specific resource making the emergency call. The dispatcher can immediately reserve a voice channel for the duration of the emergency.

Responding to an Emergency Call

A dispatcher can bypass the standard console interface to auto-open a quick list, which contains specific controls for recognizing an emergency call, initiating an emergency call, and ending an emergency call (Auto-Open of Quick List). The dispatcher can then recognize the emergency call, which ends the audible emergency indication and notifies all dispatchers that the emergency is being addressed (Emergency Recognize).

The audible emergency indication may also be muted by a dispatcher without recognizing the emergency alarm (Mute Tones at a Single Op). This can be used in a situation where one agency is monitoring a channel that belongs to another agency. That channel can be configured to not generate audible and/or visual emergency indications.

Ending an Emergency Call

When an emergency is over, the dispatcher can end the Emergency Alarm. The visual indication on the dispatch position GUI is removed, and the console informs the other dispatch positions that the emergency is over (Emergency End/ Knockdown). The emergency mode remains active on the initiating radio unit until it is ended (reset) by the radio user.

1.3.6 Radio Patch Control

The dispatcher can patch communication between trunked and/or conventional radios that are normally unable to communicate with each other due to different features, programming, or even different frequency bands. A patch group is a group of linked resources that can both receive messages from a console and transmit to all other members of the patch group.

Setting up a Standard Patch

Patches are supported between trunked resources and/or conventional resources. After the patch is created, the dispatch position transmits all audio on one resource to all other resources in the patch group. In a patch between trunked resources, patched radio users with displays see the ID or alias of the other patched radio(s), as opposed to that of the console. This minimizes confusion and the need for the dispatcher to intervene in the call. Patches are automatically reestablished, if interrupted, so the dispatcher can concentrate on continuing operations.

Predefined Patches

Patches can be predefined and automatically reinitiated each time a dispatch position computer is restarted (Patch Auto-Start).

1.3.7 Call Management and Control

The dispatcher can use the following functionality to manage and control audio for different types of calls between the dispatch position and radio users or other dispatchers.

Automatic Prioritization of Calls

Calls on the dispatch position are prioritized through a transmission hierarchy. Calls from primary supervisors take priority over those from secondary supervisors, which in turn take priority over non-supervisors. Instant Transmit or All-Points Bulletin (APB) transmissions, regardless of whether they are from a supervisor, take priority over general or patch transmissions.

Multiple dispatchers can be designated as primary supervisors on the same system, which is useful when multiple agencies share one system. With the Network Manager Client installed, supervisors can disable and enable dispatch console functionality as needed.

Manual Prioritization of Calls

System Access Priority Select allows a dispatcher to prioritize trunked resources on the system as either normal or tactical. A dispatcher can change the priority of a trunked resource to tactical to give the resource a better chance of gaining communication access on a busy system. Only emergency calls have a higher priority than tactical.

When the System Access Priority Select status of a resource is changed, it is updated at all dispatch consoles in the systems that are monitoring that trunked resource.

Using the Multi-Select Feature

The Multi-Select feature allows a dispatch position to define groups of selected radio resources. When a Multi-Select group is opened, all of the resources in the group are simultaneously selected. Resources can be added or removed from a Multi-Select group while the group is open. The dispatcher can transmit on several resources simultaneously or can listen to multiple resources simultaneously in their headset or select speakers.

Standard Call Indications

The dispatch position indicates the availability of any given resource, regardless of whether the resource is involved in a transmission. An inbound call indication provides the dispatcher with a visual cue of audio activity on a radio resource and allows a dispatcher to see at a glance what the status of a resource is at any moment.

Call Alerting

A dispatcher can use Call Alert to page an unattended radio or dispatch position through a series of beeps and an indication of the sender's ID. When available, the radio user or dispatcher sees the unit ID of the calling dispatch console or radio ID and is able to return the call.

Additionally, a Call Alert can trigger an activity. For instance, a Call Alert may cause a vehicle's horn to sound and its lights to flash. The dispatcher can even send a Call Alert to a user who is involved in voice and data communications over the network.

1.3.8 Enhanced Integrated Instant Recall Recorder (IRR)

The Enhanced IRR is seamlessly integrated with the dispatch position's software, allowing audio and call data from any radio or telephony resource to be recorded and easily played back. Call data includes PTT IDs, name of resource, start time and date, and stop time and date. Two analog inputs are available for use with recording audio from external devices.

1.3.9 MKM 7000 Console Alias Manager (CAM)

The MKM 7000 Console Alias Manager (CAM) manages the radio unit ID aliases displayed on dispatch positions. It enables agencies that share a radio system to change aliases displayed on their dispatch positions and logging recorders without affecting the aliases displayed at the other agencies on the system.

A typical console uses many types of aliases to provide meaningful, descriptive names instead of numeric ID numbers for different resources on the console, such as:

- Trunking talkgroups and conventional channels
- Aux I/Os
- Secure keys used for voice encryption
- Frequencies on multi-frequency conventional channels
- Private Line (PL) codes on conventional channels
- Predefined pages
- Radio unit IDs (also called radio PTT IDs)

The CAM supports aliases for radio unit IDs on ASTRO® 25 trunking systems, ASTRO® 25 conventional systems, MDC 1200 conventional systems,

1.4 Protecting Consoles and Communications

The console enables end-to-end encryption from the dispatcher to the ASTRO® 25 network, so that communications will not be undermined by unencrypted transmissions. Each dispatcher is able to fully participate in secure communications while being confident that sensitive, vital information is not heard by unauthorized individuals.

1.4.1 Secure Access to the Console

To use the dispatch position, a dispatcher must enter a valid radio system user account name and password. The dispatch position validates that information with the radio system's network manager and allows the dispatcher to access only the resources for which the user has access rights. This also applies to third-party applications that use the dispatch console's API.

1.4.2 Secure Communications at the Console

The console encrypts and decrypts radio voice messages. Thus, radio voice messages are encrypted from end-to-end between the radio user to the dispatch position. The dispatcher can choose whether

to encrypt their transmissions on a particular trunked resource. Dispatchers can interface with agencies that have different encryption configurations without any manual intervention or delay.

- The AXS Console supports multiple encryption algorithms and multiple secure keys (see equipment list for encryption options included).
- The dispatchers may talk and listen on radio resources which have different encryption algorithms without any manual intervention or delay.

The key material for performing audio encryption and decryption is stored locally on the console. This key material is also associated with a Common Key Reference (CKR), so that the appropriate key can be selected for a given talkgroup or a special call type.

1.5 Dispatch Console Solution Components

The proposed components are connected together and to the rest of the ASTRO® 25 system on an IP network through console site routers and switches. The console functions as an integrated component of the total radio system and fully participates in system-level features, such as end-to-end encryption.

The console connects directly to the radio system's IP transport network. Audio processing, encryption, and switching intelligence for dispatch are performed within each software-based dispatch position without additional centralized electronics.

Since the network is IP-based, the system interfaces and components can be distributed physically throughout the network. Some of the available console components are identified below.

1.5.1 CommandCentral AXS Dispatch Console Operator Position

The dispatch position supports multiple peripheral accessories, **(See equipment list section for all accessories proposed)**.



Figure 1-3: CommandCentral AXS Dispatch Console Accessories Example

Computer Display

The dispatch position will use a 22" Computer Display Touch Screen.

B1956 CommandCentral Hub (CC Hub)

The B1956 CommandCentral Hub supports the AXS dispatch console. The hub contains a workstation class computer motherboard, a 13 port USB hub and a number of analog inputs and outputs for connecting various devices. A dispatch console is capable of supporting a single CommandCentral Hub.

Desktop Speakers

Audio speakers have been included with each dispatch position and can be configured to transmit audio from a specific talkgroup or set of talkgroups. Each speaker is a self-contained unit, with individual volume controls, and can be placed on a desktop or mounted on a rack or computer display.

USB Microphone

The microphone controls the dispatch position's general transmit and monitor features through two buttons on its base. The microphone can be fastened down or left loose. It can be used alone or in conjunction with a headset.

Headset Jack

The dispatch position supports up to two headset jacks, both push-to-talk (PTT) and non-PTT-enabled, for simultaneous use by the dispatcher and a supervisor. The headset jack contains two volume controls for the separate adjustment of received radio and telephone audio.

Headset

The proposed headset consists of two elements. The headset base includes an audio amplifier, a Push-to-Talk switch, and a long cord that connects to the dispatch position. The headset top consists of the earpiece and microphone as well as a short cable that connects to the headset base.

Redundant Ethernet Connection

The optional redundant Ethernet connections increase console availability by protecting against the loss of multiple dispatch positions. In the event of a LAN switch failure, the system will automatically detect and switchover with no manual intervention required. Dispatching operations will not be interrupted.

1.6 Conventional Channel Gateways

The Conventional Channel Gateway (CCGW) is part of the core networking equipment used with the AXS Dispatch Console to provide the dispatchers access to analog conventional stations in their system. The CCGW allows an analog conventional base station, audio source, or digital channel to connect to the IP transport network and the console system. When the base stations with gateways are connected to the network, dispatchers are able to monitor and transmit on the radio channel.

The proposed system includes (2) CCGW's which are proposed to support up to eight control interfaces each. Those will interface to customer's existing conventional resources and consolettes.

1.7 Spares

Spares have been included in this proposal to be used as backups to the proposed console system (see equipment list section).

1.8 Logging Interface

The proposed offering includes an Archiving Interface server and a Firewall to interface with a Customer Supplied trunked logging recorder. For this proposal Motorola is supplying a workstation running the Windows 10 OS that will be loaded with the Motorola software to create the Archiving Interface Server.

The Archiving Interface Server (AIS) provides an interface between the radio system and a 3rd party logging recorder. The AIS provides flexible, high-quality archiving services for audio and data associated with various types of calls and events associated with radio resources. The AIS is a server which allows an IP-based logging recorder to “log onto” the radio system and request IP talkgroup and IP conventional channel audio be directed to it for recording. Once configured by the logging recorder, the AIS sends the audio and any information associated with the call to the recorder.

The user can configure the IP Logging Recorder to monitor and record a set of radio system resources (IP trunked or IP conventional). The AIS monitors the identified resources, passes call-control information to the logging sub-system via an API, and redirects audio for those monitored channels to the logging sub-system via the LAN. The logging recorder then records this information to its storage media.

The AIS is comprised of a personal computer and a Voice Processing Module (VPM). Both the PC and the VPM have separate connections to the console site LAN switch. The VPM communicates with the AIS PC via Ethernet. There is no direct physical connection between the VPM and the PC.

Secure calls can be handled in one of two ways in a radio system that employs encryption. The AIS can be configured to decrypt a secure call and pass the clear audio to the recorder along with the call control information. Or, it can be configured to only pass the call control information to the recorder and not pass any audio. This configuration is under the control of the customer.

1.9 Archiving Interface Server

1.9.1 Archiving Interface Server Equipment Overview

The proposed offering includes one AIS server that is to be installed on the console LAN. The AIS includes the following equipment:

- Computer workstation that will interface to the dispatch site switch.
- Voice Processing Module (VPM) that will also interface to the dispatch site switch.
- The AIS equipment will be rack-mounted in the proposed rack.
- Motorola has included a rack mounted KVM drawer.
- All talkgroups will be directed to the AIS via the customer provided connection from Master Site to the proposed dispatch site AIS. No additional connectivity to the Master site will be required.

A firewall is also required. Motorola has included a Firewall for the interface between the AIS and the Customer supplied trunked logging recorder. This firewall will be set up in accordance to the requirements set forth by the logging vendor. Motorola has only included the firewall required between the radio dispatch computer network and the network that will have the logging recorder.

1.9.2 Archiving Interface Server Session Limitations

The AIS functions as a trunked resource, much like a trunking RF site. The number of radio resources the AIS is programmed to record can exceed its simultaneous transmissions capacity, just like the number of talkgroups at an RF site can exceed the number of channels available at the site. The difference between the two is that the AIS begins to shed transmissions based on the priority of the transmissions whereas the trunking system busies transmissions when the capacity of the RF site is exceeded. No indication to the talking parties is provided if a transmission is shed. If shedding transmissions is not acceptable, then the number of resources the AIS is programmed to record should not exceed the capacity of the server.

If both clear and encrypted talkgroups are present in a VPM-based AIS, the AIS overall capacity is defined by the algorithm with the lowest capacity. The following formula governs the **simultaneous** processing capacity of the AIS:

$$(\# \text{ of clear calls}) + 2 \times (\# \text{ of encrypted calls}) \leq 120$$

The (# of encrypted calls) must be less than or equal to the lowest capacity limit of the algorithms that are present in the AIS.

1.9.3 Archiving Interface Server Application Programming Interface (API)

The AIS is used with a 3rd party logging recorder system. The interaction between the AIS and the recorder system is based on an Application Programming Interface (API) designed by Motorola. Motorola understands that the logging vendor. The recorder system uses the API to specify which talkgroups it wishes to record. The AIS uses the API to pass call control information and vocoded audio packets associated with radio calls to the recorder system via the LAN for storage and retrieval.

Keeping the audio in its vocoded format allows the recorder to store it in the exact form in which it was passed through the radio system. This completely eliminates any degradation of the audio quality due to compression techniques used by most recorder vendors.

Supported Call Types and Events

The following types of radio system calls are capable of being processed via the AIS:

- Trunking Talkgroup Call
- Trunking Announcement Group Call
- Trunking Emergency Call

The following types of trunking radio system events are capable of being processed via the AIS:

- Emergency Alarm
- Emergency Acknowledge
- Emergency Knockdown
- Repeater On/Off

- System Access Priority Selection (Tactical/Normal)

NOTE: The customer is responsible for working with their logging vendor to interface to the AIS using the API to meet their logging requirements and any other information logged in addition to the audio.

The logging recorder equipment and services, in addition to the ASTRO Logging Application Programming Interface (API) and Software Developer Kit (SDK) license are required to be purchased separately by logging recorder vendors.

1.9.4 Firewall

Motorola is providing a firewall to separate the AXS network LAN from the Customer provided LAN that will host the Customer supplied trunked logging recorder. The Customer Enterprise Network (CEN) firewall is a firewall that is installed in the CEN to allow communications with the ASTRO Radio Network Infrastructure (RNI).

Typically, the CEN firewall is deployed by a customer to protect their network from other networks. The firewall will be configured for network address translation (NAT) functionality. This eliminates conflicts between CEN IP addresses and RNI IP addresses. The firewall will also be configured to only pass dispatch console related traffic to and from the customer network. The firewall will communicate with the Control Room firewall via IPsec. If the customer does not have network management elements, then a local host file must be populated with the ASTRO Element FQDN (Fully Qualified Domain Name) and CEN IP address.

1.10 DSC 8000 Site Controller

The DSC 8000 Site Controller supports site conventional operation where a Conventional Channel Gateway (CCGW) is located at a dispatch console site. If the link between the console site and the zone core site is lost, the DSC 8000 enables dispatchers to communicate over conventional resources.

1.11 MC Edge Aux I/O

The Mission Critical EDGE (MC-EDGE®) as a general-purpose Remote Terminal Unit (RTU) enables users to remotely control and monitor end node devices. MC-EDGE may be deployed both indoors and outdoors in industry SCADA systems; in national infrastructure systems; in the water, oil, gas, and electricity sectors; for use with pumps or sirens; as part of a Smart City; and in modern IoT ecosystems connected to the Cloud.

1.12 Assumptions

- Existing conventional resources will be reused and no new consolettes, antenna or lines are provided.
- This proposal does not include any control station combiners.
- This proposal does not include any loggers. The logging recorder solution will be provided by the customer.
- Headsets, headset Jacks, headset bases and footswitches will be reused from the (5) existing consoles.

- The racks provided will house the proposed equipment in this proposal. Any additional equipment that the customer has existing or will bring it over to the dispatch, it may require an additional rack. If additional rack is required, a change order may be executed.
- This proposal does not include any furniture for the new dispatch. It is the customer's responsibility to provide furniture for the new dispatch site.
- Customer is responsible for connecting this new dispatch site to the core. Motorola has not provided any backhaul equipment or MPLS equipment to setup the connectivity back to the core.
- The MC Edge Auxiliary I/O provided has capacity for 48 inputs and 24 outputs. If more I/Os are required, then a change order will be separately required.
- This proposal includes (2) MCG 8000s to interface to the existing conventional resources and consolettes provided by the customer. If more conventional channel gateways are required, then a change order will separately be required.

Section 2

Equipment List

Item No.	Qty	Nomenclature	Description
1	1	SQM01SUM0323A	ASTRO MASTER SITE
2	1	CA03517AF	ASTRO CORE EXPANSION, AN2024.X
3	2	UA00156AA	ADD: 5 CONSOLE OPS: AXS, MCC7500/E AND AIS
4	2	CA01316AA	ADD: UNC ADDTL DEVICE LIC (QTY 10)
5	7	HKVN4729A	AXS DISPATCH CONSOLE LICENSE
6	7	HKVN4730A	LICENSE, AXS TRUNKING SERVICES LICENSE
7	7	HKVN4731A	LICENSE, AXS ADVANCED CONVENTIONAL SERVICES LICENSE
8	7	HKVN4732A	LICENSE, AXS SECURE VOICE SERVICES LICENSE
9	7	HKVN4733A	LICENSE, AXS INTEGRATED IRR
10	7	HKVN4736A	LICENSE, AXS AMBE+2 VOCODER ROYALTY AND LICENSE
11	7	HKVN4737A	LICENSE, AXS STANDARD LEVEL RADIO RESOURCE CAPACITY LICENSE
12	1	B1957A	AXS SOFTWARE DVD
13	7	B1956A	COMMANDCENTRAL HUB, W/CLIENT PC
14	7	CA03850AA	ADD: WINDOWS OS FOR MCC7500E CONSOLE
15	7	CA03553AA	ADD: AC LINE CORD, NORTH AMERICA
16	7	CA03547AA	ADD: BRACKET, MOUNTING 2RU
17	7	CA03583AA	ADD: FOUR CABLES, POWER 24VDC
18	7	CA03572AA	ADD: CABLE RETENTION BRACKET
19	7	B1951B	MICROPHONE, DESKTOP, USB
20	7	CA03413AA	ADD: USB CABLE, TYPE A TO TYPE C, 4.5M
21	28	B1952B	SPEAKER, DESKTOP, USB
22	28	CA03413AA	ADD: USB CABLE, TYPE A TO TYPE C, 4.5M
23	7	L3226A	CERTIFIED OPTICAL WHEEL MOUSE FOR RSD SERVERS AND WORKSTATIONS
24	7	L3225A	CERTIFIED KEYBOARD FOR RSD SERVERS AND WORKSTATIONS
25	1	DSF2B56AA	USB EXTERNAL DVD DRIVE
26	7	DSEV221B	TECH GLOBAL EVOLUTION SERIES 22INCH WITH TOUCH
27	9	T8742A	MCAFFEE FOR WINDOWS CLIENT, A2019.2 +PLUS
28	9	T8807A	WINDOWS SUPP FULL CONFIG, A2022.1
29	2	TDN9841A	MOUSE PADS 5 PACK
30	9	DSACPS6N120SN2TT	AC POWER STRIP, 6 OUTLETS, SASD PROTECTED, UL1449/R56, 12FT CORD
31	1	BVN1013A	MKM 7000 CONSOLE ALIAS MANAGER SOFTWARE
32	1	TT4270A	Z2 G9 MINI WORKSTATION NON-RETURNABLE

Item No.	Qty	Nomenclature	Description
33	1	T8810A	STANDALONE DSC 8000 CONTROLLER
34	1	CA04079AA	ADD: ASTRO NEXT SYSTEM RELEASE 2024.X
35	1	CA03801AA	ADD: DSC 8000 CONVENTIONAL SITE CONTROLLER
36	1	UA00787AA	ADD: DSC 8000 CONVENTIONAL SITE CONTROLLER SW
37	1	CA03832AA	ADD: NM--DISPATCH SITE
38	1	T8811A	DSC AC POWER SUPPLY CHASSIS
39	1	CA03800AA	ADD: SINGLE POWER SUPPLY FOR DSC
40	1	CA03533AA	ADD: DSC AC POWER CABLE - US, 12 FT
41	2	SQM01SUM0333A	MCG 8000 CONVENTIONAL GATEWAY
42	2	CA03714AA	ADD: AC POWER
43	16	CA03717AA	ADD: ACIM INTERFACE
44	8	CA03719AA	ADD: DIGITAL IP INTERFACE
45	8	CA03720AA	ADD: ANALOG IP INTERFACE
46	2	TRN7343A	RACK 7.5'
47	2	DDN9748A	19 INCH BLACK SHELF
48	2	DS11011188	PDU, 120/240 SPLIT PH OR N+1 REDUNDANT, 60A MAX PER PHASE, SIX DEDICAT
49	26	DS3750297	BREAKER, 15 AMP, CB UL 489 LISTED FOR AC EDGE II (1101-1188)
50	4	DS1101990	SPD, SHIELDED RJ-45 JACK, SINGLE LINE GBE (1000MBPS) R56 COMPLIANT
51	4	DSTSJADP	RACK MOUNT GROUND BAR, 19 IN FOR TSJ AND WPH SERIES DATA SPDS
52	2	T8492A	SITE ROUTER & FIREWALL- AC
53	2	CA03445AA	ADD: MISSION CRITICAL HARDENING
54	2	CA03448AA	ADD: STATEFUL FIREWALL
55	2	CA03446AA	ADD: ENCRYPTION
56	2	CLN9066A	SWITCH, SWITCH, EX4100 24-PORT SWITCH NON TAA
57	2	CLN9105A	FRU: JUNIPER 1M DAC CABLE
58	1	F0016A	MC IOT MAIN MODEL
59	1	VA01945AA	ADD: MC EDGE AS AUX I--O SERVER
60	1	VA00985AA	ADD: NO PIGGY_ MC-EDGE
61	1	VA00147AA	ADD: FRONT CABLE COVERS
62	3	VA00989AA	ADD: MIXED DIGITAL _ 8DO EE 16DI 5-18 V --DRY
63	1	VA00009AA	ADD: AC POWER SUPPLY 12V--120W DC OUT
64	1	VA00155AA	ADD: DC POWER CABLE
65	18	FKN0044A	MC_EDGE MIGRATION CABLE
66	1	VA00153AA	ADD: I--O MODULE EXTRACTOR TOOL
67	1	VA00341AA	INC:MC-EDGE MAIN FILE SYSTEM
68	1	VA00142AA	INC: EXTREMDB LICENSE
69	3	VA00049AA	INC: I--O MODULE CABLE COVER

Item No.	Qty	Nomenclature	Description
70	1	VA00974AA	INC: IOT MC-EDGE CPU PACKAGE
71	1	VA00442AA	INC:MC-EDGE SYSTEM SW FILES
72	1	VA00967AA	INC: CPU PACKING
73	1	VA01383AA	INC: FRONT CABLE COVERS FOR MC EDGE
74	1	FHN0057A	DIN RAIL STOPPER
75	1	DSIABDIN4	PANDUIT IABDIN4 4 RACK UNIT DIN RAIL FOR EIA 19" MOUNT
76	3	FHN1668A	TERM BLOCK & CONN WIRED M25T68L
77	1	B1933A	MOTOROLA VOICE PROCESSOR MODULE
78	1	CA00147AF	ADD: MCC 7500 SECURE OPERATION
79	1	CA00288AB	ADD: MCC 7500 AIS SOFTWARE LICENSE
80	1	CA00143AC	ADD: DES-OFB ALOGRITHM
81	1	CA00182AB	ADD: AES ALOGRITHM
82	1	CA00245AA	ADD: ADP ALGORITHM
83	1	CA00140AA	ADD: AC LINE CORD, NORTH AMERICAN
84	1	BLN1297A	VPM POWER SUPPLY MOUNTING KIT
85	1	TT4270A	Z2 G9 MINI WORKSTATION NON-RETURNABLE
86	1	T8639A	JUNIPER CONTROL ROOM FIREWALL
87	1	T8669A	JUNIPER CONTROL ROOM FIREWALL RECOVERY MEDIA
88	1	CLN9066A	SWITCH, SWITCH, EX4100 24-PORT SWITCH NON TAA
89	1	DSB07001619	TRIPP LITE 16 PORT RACK CONSOLE KVM S 19IN RACKMOUNT SWITCH
90	2	DSB078101USB1	USB SINGLE SRVR INTERFACE UNIT VIRTUAL MEDIA KVM SWITCH HD15 USB RJ4
91	4	B1913A	MCC SERIES HEADSET JACK
92	4	RLN6098A	HDST MODULE BASE W/PTT, 15 FT CBL
93	4	RMN5150A	OVER-THE-HEAD, MONAURAL, NOISE-CANCELING HEADSET
94	2	DSTWIN6328A	PROVIDES ONE DUAL PEDAL FOOTSWITCH
Spares			
95	1	B1956A	COMMANDCENTRAL HUB, W/CLIENT PC
96	1	CA03850AA	ADD: WINDOWS OS FOR MCC7500E CONSOLE
97	1	CA03553AA	ADD: AC LINE CORD, NORTH AMERICA
98	1	CA03547AA	ADD: BRACKET, MOUNTING 2RU
99	1	CA03583AA	ADD: FOUR CABLES, POWER 24VDC
100	1	CA03572AA	ADD: CABLE RETENTION BRACKET
101	1	B1913A	MCC SERIES HEADSET JACK
102	1	B1951B	MICROPHONE, DESKTOP, USB
103	1	CA03413AA	ADD: USB CABLE, TYPE A TO TYPE C, 4.5M
104	1	B1952B	SPEAKER, DESKTOP, USB
105	1	CA03413AA	ADD: USB CABLE, TYPE A TO TYPE C, 4.5M

Item No.	Qty	Nomenclature	Description
106	1	CA03405AA	ADD: POWER SUPPLY WITH DC CORD
107	1	CA03406AA	ADD: AC LINE CORD, NORTH AMERICA
108	1	L3226A	CERTIFIED OPTICAL WHEEL MOUSE FOR RSD SERVERS AND WORKSTATIONS
109	1	L3225A	CERTIFIED KEYBOARD FOR RSD SERVERS AND WORKSTATIONS
110	1	RLN6098A	HDST MODULE BASE W/PTT, 15 FT CBL
111	1	DSTWIN6328A	PROVIDES ONE DUAL PEDAL FOOTSWITCH
112	1	T8492A	SITE ROUTER & FIREWALL- AC
113	1	CA03445AA	ADD: MISSION CRITICAL HARDENING
114	1	CA03448AA	ADD: STATEFUL FIREWALL
115	1	CA03446AA	ADD: ENCRYPTION
116	1	CLN9066A	SWITCH, SWITCH, EX4100 24-PORT SWITCH NON TAA
117	1	SQM01SUM0333A	MCG 8000 CONVENTIONAL GATEWAY
118	1	CA03714AA	ADD: AC POWER
119	1	CA03719AA	ADD: DIGITAL IP INTERFACE

Section 3

Statement of Work

3.1 Overview

Motorola proposes the installation and configuration of the equipment defined in the System Description and Equipment List. The document delineates the general responsibilities between Motorola and City of Gahanna, Ohio ("Customer") as agreed to by contract.

The proposed system connects to the Ohio MARCS system.

NOTE: All responsibilities which are noted as City of Gahanna responsibilities are items which the City must complete or ensure that Ohio MARCS will provide. In addition, City of Gahanna is responsible for providing all approvals and memorandums of understanding, as needed, from Ohio MARCS to Motorola.

3.1.1 Motorola's Responsibilities

Motorola's general responsibilities include the following:

- Conduct project kickoff meeting with the City to review project design and finalize requirements.
- Schedule the implementation schedule in agreement with the City. Coordinate the activities of all Motorola subcontractors under this contract.
- Provide the City with the appropriate system interconnect specifications.
- Define link specifications for each link required for the proposed system.
- Define electrical requirements for each equipment rack and operator position to be installed in City of Gahanna provided facilities.
- Define heat load for each equipment rack to be installed in City of Gahanna-supplied facilities.
- Administer safe work procedures for installation.
- Install the new console operator position(s) in the location and on desktop space provided by City of Gahanna.
- Convert existing (5) MCC 7500 operator positions to AXS operator positions and install at the new dispatch site
- Install the (2) new AXS operator positions at the customer provided new dispatch site.
- Install the backroom equipment rack with auxiliary networking equipment (routers, switches) as needed at the main dispatch to interface to the MARCS system.
- Install the new DSC 8000 site controller with power supply in the proposed backroom dispatch site rack of equipment
- Reuse all existing conventional resources to be separately provided and installed, programmed by the Customer.
- Install and configure the proposed new Console Alias Manager
- Install and configure the proposed new AIS and Firewall.

- Connect the console(s) to the existing Customer-provided circuits.
- If existing, utilize pre-wired auxiliary input/outputs to the proposed Motorola Edge auxiliary input/output box, as applicable

NOTE: If any new wiring for input/outputs is needed at the dispatch site an additional quote can be provided.

- Install cabling to connect the backroom equipment to the new dispatch consoles.
- Connect the appropriate equipment to customer-supplied ground system in accordance with Motorola's R56 Site Installation Standards.
- Perform the console programming, based on the console templates designed during the fleetmapping process jointly by Motorola and the City of Gahanna.
- Provide removal of existing customer owned (5) operator position console equipment from the MECC dispatch location after cutover is complete.
- Deliver removed console equipment to customer designated location.
- Connect City of Gahanna-supplied, previously identified circuits into the console, to a demarcation point located within 25 feet of the console interface.

NOTE: Motorola is not responsible for interference caused or received by the Motorola-provided equipment except for interference that is directly caused by the Motorola-provided transmitter(s) to the Motorola-provided receiver(s). Should the City's system experience interference, Motorola can be contracted to investigate the source and recommend solutions to mitigate the issue.

- Integration of other third-party products, not defined in this statement of work, is not included in this proposal.
- Optimize equipment and verify that all equipment is operating properly and that all electrical and signal levels are set accurately.
- Verify communication interfaces between devices for proper operation.
- Test features and functionality are in accordance with manufacturers' specifications.
- Verify the operational functionality and features of the dispatch subsystems and the system supplied by Motorola, as contracted.
- If any major task as contractually described fails, repeat that particular task after Motorola determines that corrective action has been taken.
- Document all issues that arise during the acceptance tests.
- Document the results of the acceptance tests and present to City of Gahanna for review.
- Resolve any punchlist items before Final System Acceptance.
- Final System Acceptance shall be deemed successful when the ATP tests pass. The Customer and Motorola Solutions mark the event by signing and dating the Final System Acceptance milestone certificate.

3.1.2 City of Gahanna Responsibilities

The Customer will assume responsibility for the installation and performance of all other equipment and work necessary for completion of this project that is not provided by Motorola. The City of Gahanna's general responsibilities for both the dispatch location and the Ohio MARCS Zone Core site are as follow:

- Customer will provide a dedicated delivery point for receipt, inventory, and storage of equipment prior to installation.
- Coordinate the activities of all City of Gahanna vendors or other contractors, if applicable.
- Attend and participate in project meetings and reviews.
- Provide ongoing communication, as applicable, with Ohio MARCS regarding the dispatch console project and schedule.
- Provide existing MCC 7500 dispatch site with backroom rack and network equipment at the current Ohio MARCS system release version.
- Provide existing, (5) MCC 7500 operator positions with accessories for conversion and reuse, as applicable.
- Provide all wiring for the Auxiliary input/outputs and all conventional resources, as applicable.
- Provide dispatch facility and antenna mounting locations as required for dispatch sub-system installation.
- Provide all installed/programmed control stations/consolettes (up to 16) with antenna and line and cabling to the backroom which can interface to the Motorola gateways in the backroom equipment rack.

NOTE: All antenna and line installation heights are assumed to be <20 feet. If greater than 20' any FCC licensing requirements are the responsibility of the Customer. In addition, roof penetration, core drilling, and/or tower crew, bucket truck requirements for installations of antenna and line are not proposed.

- Provide logging recorder equipment and all associated services, including removal, re-location/installation and configuration, and the Motorola API, SDK, as needed.
- Ensure communications sites meet space, grounding, power, and connectivity requirements for the installation of all equipment.
- Obtain all licensing, site access, or permitting required for project implementation.

Restrictions:

- Motorola assumes no liability or responsibility for inadequate frequency availability or frequency licensing issues.
- Motorola is not responsible for issues outside of its immediate control. Such issues include, but are not restricted to, improper frequency coordination by others and non-compliant operation of other radios.
- Motorola is not responsible for co-channel interference due to errors in frequency coordination by APCO or any other unlisted frequencies, or the improper design, installation, or operation of systems installed or operated by others.
- If, for any reason, any of the proposed sites cannot be utilized due to reasons beyond Motorola's control, the costs associated with site changes or delays including, but not limited to, re-engineering, frequency re-licensing, site zoning, site permitting, schedule delays, site abnormalities, re-mobilization, etc., will be paid for by the Customer and documented through the change order process.
- Secure site lease/ownership, zoning, permits, regulatory approvals, easements, power, and Telco connections.
- Provide third party products and interface if needed.
- Provide demarcation point located within 25 feet of the console interface.

- Provide clear and stable access to the sites for transporting electronics and other materials. Sufficient site access must be available for trucks to deliver materials under their own power and for personnel to move materials to the facility without assistance from special equipment.
- Supply adequately sized electrical service, backup power (UPS, generator, batteries, etc.) including the installation of conduit, circuit breakers, outlets, etc., at each equipment location. Provide AC power (dedicated 20 Amp AC outlets—simplex with ground) for each major piece of equipment within six (6) feet of the location of the Motorola-supplied equipment, including the associated electrical service and wiring (conduit, circuit breakers, etc.).
- Provide adequate HVAC, grounding, lighting, cable routing, and surge protection (also, among existing and Motorola-provided equipment) based upon Motorola's "Standards and Guidelines for Communication Sites" (R56). Ceiling [minimum nine (9) feet] and cable tray heights [minimum eight (8) feet] in the equipment rooms in order to accommodate seven (7)-foot, six (6)-inch equipment racks.
- Bring grounding system up to Motorola's "Standards and Guidelines for Communication Sites" (R56) and supply a single point system ground, of five (5) ohms or less, to be used on all FNE supplied under the Contract. Supply grounding tie point within 10 feet from the Motorola-supplied equipment.
- Provide floor space and desk space (including desk furniture, as needed) for the system equipment at Customer-provided facilities. Each rack shall be provided a minimum of 24-inch x 24-inch footprint with 36 inches clearance in the front and back.
- Relocate and/or removal of existing equipment, if needed, to provide required space for the installation of Motorola-supplied equipment.
- Provide obstruction-free area for the cable run between the demarcation point and the communications equipment, as well as between the backroom equipment room and dispatch positions.
- Supply interior building cable trays, raceways, conduits, and wire supports.
- Resolve any environmental issues including, but not limited to, asbestos, structural integrity of the site, and any other building risks (resolve environmental or hazardous material issues).
- Provide console template and alias information as required for programming.
- Pay for usage costs of power and generator fueling, both during the construction and installation effort, and on an ongoing basis.
- Any required system network link resources will be provided by City of Gahanna, per Motorola specifications for consoles to connect to the Ohio MARCS master site.
- Provide connectivity test results to confirm specification compliancy prior to equipment installation.
- Layer 3 MPLS equipment is recommended for all links.
- Provide 24-hour test compliance, per Motorola specification.
- Provide IT contact representative for backhaul related requirements

NOTE: Links may include dedicated phone circuits, microwave links, or other types of connectivity.

- Provide space for console cutover.
- Provide designated location for existing console equipment to be stored after removal.

3.2 Project Schedule

Motorola's preliminary schedule indicates total project implementation to be approximately 10-14 months pending supply chain availability at time of purchase, completion of customer deliverables including civil work and site development. This preliminary schedule is included for informational purposes only and assumes that all City of Gahanna responsibilities as defined above are completed, as required. If site improvements or site approvals are needed these must be completed prior to equipment shipping to the field.

Section 4

Warranty & Maintenance Plan

4.1 Warranty Support Services

The Year 1 services include the Advanced Plus services noted below for the proposed new equipment only.

NOTES: MDR is proposed for the proposed new offering. All Ohio MARCS system add-ons require security monitoring or MDR. The availability of MDR is pending the conversion of Ohio MARCS to MDR monitoring.

Services proposed for add-on equipment assumes and requires that the existing sites / system to separately include and be contracted for the same services for the same duration.

NOTE: Post warranty infrastructure lifecycle services are optionally provided and include the same services as offered during year 1 as described in the lifecycle services section below. See optional pricing noted within the pricing section.

As an Add on to Ohio MARCS all add-ons are required to align with the regular MARCS System Upgrade schedule through 2039 and must include security monitoring and security update services. The post warranty services include these MARCS required services.

4.2 ASTRO 25 Advanced Plus Services Statement of Work

4.2.1 Overview

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

Advanced Plus Services consist of the following elements:

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

- Annual Preventative Maintenance
- System Upgrade Agreement (SUA)

Each of these elements is summarized below and expanded upon in **Error! Reference source not found.**: Advanced Plus Services Detailed Description. In the event of a conflict between the descriptions below and an individual subsection of **Error! Reference source not found.**: Advanced Plus Services Detailed Description, the individual subsection prevails.

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

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

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

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

ASTRO System Monitoring

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

- Managed Detection and Response

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

- Network Event Monitoring

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

- ASTRO Connectivity Service

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

Remote Technical Support

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

Network Hardware Repair

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

Security Update Service

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

Remote Security Update Service

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

On-Site Infrastructure Response

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

Annual Preventive Maintenance

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

System Upgrade Agreement

Utilizing the ASTRO 25 System Upgrade Agreement (SUA) service, the ASTRO 25 system is able to take advantage of new functionality and security features while extending the operational life of the system. Motorola continues to make advancements in on-premises and cloud technologies to bring value to our customers. Cloud technologies enable the delivery of additional functionality through frequent updates ensuring the latest in ASTRO 25 is available at all times.

4.3 Motorola Service Delivery Ecosystem

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

4.4 Centralized Managed Support Operations

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

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

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

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

4.5 Field Service

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

4.6 Customer Support Manager

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

The CSP functions as an operating document that personalizes the services described in this document. The CSP contains Customer-specific information, such as site names, site access directions, key contact persons, incident handling instructions, and escalation paths for special issues. The CSP also defines the division of responsibilities between the Customer and Motorola so response protocols are pre-defined and well understood when the need arises.

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

4.7 Customer Hub

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

- **Network Event Monitoring:** Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.
- **Remote Technical Support:** Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.

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

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

4.8 Connectivity Specifications

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

4.9 Advanced Plus Services Detailed Description

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

4.10 ASTRO System Monitoring (NEW)

4.10.1 Managed Detection and Response

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

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

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

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

4.10.1.1 Description of Service

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

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

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

4.10.1.2 Managed Detection and Response Elements

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

ActiveEye Security Platform

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

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

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

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

ActiveEye Remote Security Sensor

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

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

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

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

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

Endpoint Detection and Response

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

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

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

Cloud Based Vulnerability Scan Engine

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

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

Control Room Firewall

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

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

Specification	Requirement
Rack Space	1U
Power Consumption (Max)	28.6 W (Single Power Supply)
Power Input	100-240V AC
Current	.52 A

Specification	Requirement
Circuits Breaker	Qty. 1
Heat Dissipation (Max)	97.6 BTU/hr
Line Cord	NEMA 5-15P
Internet Service Bandwidth	High availability Internet Connection (99.99% [4-9s] or higher) Packet loss < 0.5% Jitter < 10 ms Delay < 120 ms RJ45 Port Speed – Auto Negotiate

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

4.10.1.3 Deployment Timeline and Milestones

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

Phase 1: Service Onboarding

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

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

Phase 2: Infrastructure Readiness

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

Phase 3: System Buildout and Deployment

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

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

Phase 4: Monitoring “Turn Up”

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

Phase 5: Tuning and Customer Training

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

Service Commencement

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

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

4.10.1.4 General Responsibilities

Motorola Responsibilities

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

Note that network segments with insufficient connectivity to support endpoint detection and response will be considered out of scope for endpoint detection and response

- Motorola will perform the installation of endpoint detection and response agents in the RNI-DMZ CEN(s) and Control Room CEN(s) for all Motorola managed devices that support endpoint detection and response agents.

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

Customer Responsibilities

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

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

4.10.1.5 Service Modules

4.10.1.5.1 Log Collection / Analytics

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

Motorola Responsibilities

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

Customer Responsibilities

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

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

4.10.1.6 Network Detection

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

Motorola Responsibilities

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

Customer Responsibilities

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

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

4.10.1.7 Endpoint Detection and Response

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

Motorola Solutions Responsibilities

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

Customer Responsibilities

- Work with Motorola to ensure that there is a documented incident response plan that indicates how Motorola should engage with the Customer in the event of a detection of an indicator of compromise.

- Provide and maintain contact information for a Customer point of contact that can take action or authorize Motorola to take action in the event of a detection of an indicator of compromise.

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

4.10.1.8 External Vulnerability Scanning

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

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

Motorola Responsibilities

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

Customer Responsibilities

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

Applies to Internet facing assets only.

4.10.1.9 Security Operations Center Monitoring and Support

4.10.1.9.1 Scope

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

Motorola's SOC is staffed with security experts who will use ActiveEye security platform to monitor elements integrated by service modules. In addition, SOC staff will take advantage of their extensive

experience to investigate and triage detected threats, and to recommend responses to the Customer. Depending on Customer security policies and the extent to which endpoint detection and response is deployed within the system, the SOC may take actions to deploy countermeasures in an attempt to contain a security incident. Customer support is provided in the English language.

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

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

4.10.1.9.2 Ongoing Security Operations Center Service Responsibilities

Motorola Responsibilities

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

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

Customer Responsibilities

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

4.10.1.9.3 Technical Support

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

Motorola Responsibilities

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

Customer Responsibilities

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

Limitations and Exclusions

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

4.10.1.10 Incident Response

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

When an IoC is observed, the Motorola Security Operations team will engage with the customer to investigate the issue, determine the extent of the compromise and contain the activity to the extent possible with the Motorola security controls deployed within the environment. This expert guidance is available upon contract signature and extends through MDR infrastructure deployment phases and the term of the contract.

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

Motorola Responsibilities

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

Customer Responsibilities

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

4.10.1.11 Event Response and Notification

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

Table 4-1: Event Handling

Event Type	Details	Notification Requirement
False Positive or Benign	Any events determined by Motorola to not likely have a negative security impact on the organization.	None
Event of Interest (EOI)	Any events determined by Motorola to likely have a negative security impact on the organization.	Escalate to Customer in accordance with routine notification procedure. Escalate in accordance with urgent notification procedure when required by agreed-upon thresholds and SOC analysis. Notification procedures are included in Table 4-2.

4.10.1.12 Notification

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

Table 4-2: Notification Procedures

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

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

4.10.1.13 Tuning

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

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

4.10.1.14 Tuning Period Exception

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

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

4.10.1.15 Incident Priority Level Definitions and Response Times

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

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

Response Time Goals

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

ActiveEye Platform Availability

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

ActiveEye Remote Security Sensor (AERSS)

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

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

4.10.1.16 Included Services

Site Information

The following quantities are included in the scope:

Site / Location	Quantity
Primary zone cores	0
DSR backup cores	0
Sites (NMD, T-Sub, C-Sub)	0
CEN (Control Room)	1
CEN (RNI-DMZ)	0
Network Management Clients	0
Dispatch Consoles	7
AIS	1
CEN Endpoints	Up to 10

Services Included

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

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

The following table lists any ancillary components required.

Description	Quantity
Internetworking Firewall	0
Control Room Firewall	1

4.10.1.17 Limitations and Exclusions

This section applies to all cybersecurity services contained in the Statement of Work. Managed Detection and Response does NOT include services to perform physical containment and/or remediation of confirmed security incidents, remote or onsite. The Customer may choose to purchase

additional Incident Response professional services to assist in the creation of and/or execution of a Customer's Incident Response Plan.

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

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

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

Service Limitations

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

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

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

Customer and Third-Party Information

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

Third-Party Software and Service Providers, Including Resale

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

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

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

4.10.2 Network Event Monitoring

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

4.10.2.1 Description of Service

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

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

Standard Threshold	Optional Threshold
An incident will be triggered if an event fulfills one of the two following criteria: <ul style="list-style-type: none">▪ Event occurs 5 times in 30 minutes.▪ Event causes 10 minutes of continuous downtime for a monitored component.	An incident will be triggered if an event fulfills one of the two following criteria: <ul style="list-style-type: none">▪ Event occurs 7 times in 30 minutes.▪ Event causes 15 minutes of continuous downtime for a monitored component.

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

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

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

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

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

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

4.10.2.2 Scope

Network Event Monitoring is available 24/7. Incidents generated by the monitoring service will be handled in accordance with Section 4.11 Priority Level Definitions and Response Time.

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

4.10.2.3 Inclusions

Network Event Monitoring is available for the devices listed in Section 4.10.2.6: Monitored Elements.

Motorola Responsibilities

- Provide a dedicated network connection necessary for monitoring the Customer's communication network.
- Provide continuous utility service to any Motorola equipment installed or used at the Customer's premises to support delivery of the service. The Customer agrees to take reasonable due care to secure the Motorola equipment from theft or damage while on the Customer's premises.
- Create an incident, as necessary. Gather information to perform the following:

- Characterize the issue.
 - Determine a plan of action.
 - Assign and track the incident to resolution.
- Prior to contract start date, provide Motorola with pre-defined information necessary to complete a CSP, including:
 - Incident notification preferences and procedure.
 - Repair verification preference and procedure.
 - Database and escalation procedure forms.
- Submit timely changes in any information supplied to Motorola and included in the CSP to the CSM.
- Notify the CMSO when the Customer performs any activity that impacts the system. Activity that impacts the system may include, but is not limited to: installing software or hardware upgrades, performing upgrades to the network, renaming elements or devices within the network, and taking down part of the system to perform maintenance.
- Send system configuration change requests to Motorola's CSM.
- Allow Motorola's field service technician, if designated in the CSP, access to equipment, including any connectivity or monitoring equipment, if remote service is not possible.
- Allow Motorola's field service technician, if designated in the CSP, access to remove Motorola-owned monitoring equipment upon cancellation of service.
- Provide Motorola with all Customer-managed passwords required to access the Customer's system upon request, when opening a request for service support, or when needed to enable response to a technical issue.
- Pay additional support charges above the contracted service agreements that may apply if it is determined that system faults were caused by the Customer making changes to critical system parameters without written agreement from Motorola.
- In the event that Motorola agrees in writing to provide supplemental monitoring for third-party elements provided by the Customer, the Customer agrees to obtain third party consents or licenses required to enable Motorola to provide the monitoring service.
- Cooperate with Motorola and perform reasonable or necessary acts to enable Motorola to provide these services.
- Contact Motorola to coordinate transition of monitoring when the responsibility for monitoring needs to be transferred to or from Motorola, as specified in pre-defined information provided in the Customer's CSP. An example of a transfer scenario is transferring monitoring from Motorola for network monitoring after normal business hours.
 - Upon contact, the Customer must provide Motorola with customer name, site ID, status on any open incidents, priority level of any open incidents, brief descriptions of any ongoing incident, and action plan for resolving those incidents.
- Acknowledge that incidents will be handled in accordance with **Error! Reference source not found.:** Priority Level Definitions and Response Times.
- Connectivity Matrix describes available connectivity options.
- If determined necessary by Motorola, provide Motorola-owned equipment at the Customer's premises for monitoring network elements. The type of equipment and location of deployment is listed in Section 4.10.2.5: Motorola Owned and Supplied Equipment.

- Verify connectivity and event monitoring prior to system acceptance or start date.
- Monitor system continuously during hours designated in the CSP, and in accordance with Section 4.11 Priority Level Definitions and Response Time.
- Remotely access the Customer's system to perform remote diagnosis as permitted by the Customer.
- Provide the Customer with a link to access system configuration info, site info, system notifications, and system notes.
- Cooperate with the Customer to coordinate the transition of monitoring responsibilities between Motorola and the Customer.
- Maintain communication as needed with the Customer in the field until incident resolution.
- Provide available information on incident resolution to the Customer.

Limitations and Exclusions

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

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

Customer Responsibilities

- Allow Motorola continuous remote access to enable the monitoring service.
- Provide continuous utility service to any Motorola equipment installed or used at the Customer's premises to support delivery of the service. The Customer agrees to take reasonable due care to secure the Motorola equipment from theft or damage while on the Customer's premises.
- Create an incident, as necessary. Gather information to perform the following:
 - Characterize the issue.
 - Determine a plan of action.
 - Assign and track the incident to resolution.

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

4.10.2.4 Connectivity

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

Table 4-4: Available Connectivity

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

4.10.2.5 Motorola Owned and Supplied Equipment

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

Table 4-5: Motorola Owned and Supplied Equipment

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

4.10.2.6 Monitored Elements

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

Table 4-6: Monitored Elements

Monitored Elements		
Active Directory	Enrichment Testing	Probe
Agent	Environmental	Core Switch
AIS	ESX	Radio Interface
AMB	Exit Router	RDM
Application Server	RNI Firewall	RFDS
APX Cloud Application	Core Server	RGU
ATR	Gateway	RNG
AUC	Gateway Router	Site Router
Backup Server	Gateway Unit	RTU
Base Radio	GIS Server	SCOM Server
Call Processor	HSS	Short Data Router
Camera	Install Server	Statistical Server
CBSD	Site Switch	Storage Networking
CCGW	Licensing Service	Consoles
Channel	Load Balancer	TRAK
Client Station	Logging Recorder	Terminal Server
CommandCentral AXS dispatch console	Logging Replay Station	Time Keeper

Monitored Elements		
Controller	UNC	Training App
Conventional	UEM	Training Database
Core Router	MOSCAD Server	Trap Forwarder
Data Processing	Network Address	UCS
Database Server	Network Device	Licensing Server
Data Warehouse Server	NTP	Virtual Machine
Device Configuration Server	AIS	VMS
DNS	Application Server	VPM
Domain Controller	Packet Data Gateway	WSGU
D series Site Controller	Physical Host Environmental	ZDS
eNodeB	Physical Host Power and Network	Zone Controller
Active directory	Power Distribution Unit	Syslog
Repeaters	Power Monitor	Proxy

4.10.3 ASTRO Connectivity Services

To establish a connection between the Customer's on-premises ASTRO 25 infrastructure core and Motorola Solutions Network and Security Operation Centers, Motorola will provide required network equipment with sufficient bandwidth as mentioned in Section 4.10.2.5: Motorola Owned and Supplied Equipment. The connectivity to customer's ASTRO 25 infrastructure core will terminate upon the Customer canceling their ASTRO 25 service package.

Motorola Responsibilities

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

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

- Install equipment supplied by Motorola. Installation period is estimated to be within 45 business days from when Motorola and Customer execute the Agreement and related addendum or addenda.
- Cooperate with the Customer to schedule the ASTRO 25 Connectivity Service implementation.
- Administer safe work procedures for installation of the remote access circuit.

Customer Responsibilities

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

- Upon termination of the services, Customer shall promptly return to Motorola all equipment provided by Motorola in conjunction with the ASTRO 25 Connectivity Service and not explicitly owned by Customer. Motorola is entitled to invoice any and all costs arising out of or in connection with Customer's failure to return the Motorola equipment if the Motorola equipment is not returned within sixty (60) days following termination of services.

Limitations/Exclusions

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

4.10.4 Remote Technical Support

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

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

4.10.4.1 Description of Service

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

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

The CMSO Operations Center classifies and responds to each technical support request in accordance with Section 4.11 Priority Level Definitions and Response Time.

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

4.10.4.2 Scope

The CMSO Service Desk is available via telephone 24/7 to receive and log requests for technical support. Remote Technical Support service is provided in accordance with Section 4.11 Priority Level Definitions and Response Time.

4.10.4.3 Inclusions

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

Motorola Responsibilities

- Maintain availability of the Motorola CMSO Service Desk via telephone (800-MSI-HELP) 24/7 to receive, log, and classify Customer requests for support.
- Respond to incidents and technical service requests in accordance with Section 4.11 Priority Level Definitions and Response Time.
- Provide caller a plan of action outlining additional requirements, activities, or information required to achieve restoral/fulfillment.
- Maintain communication with the Customer in the field as needed until resolution of the incident.
- Coordinate technical resolutions with agreed upon third-party vendors, as needed.
- Escalate support issues to additional Motorola technical resources, as applicable.
- Determine, in its sole discretion, when an incident requires more than the Remote Technical Support services described in this SOW and notify the Customer of an alternative course of action.

Limitations and Exclusions

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

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

Customer Responsibilities

- Prior to contract start date, provide Motorola with pre-defined information necessary to complete CSP.
- Submit timely changes in any information supplied in the CSP to the CSM.
- Contact the CMSO Service Desk to engage the Remote Technical Support service when needed, providing the necessary information for proper entitlement services. This information includes, but is not limited to, the name of contact, name of Customer, system ID number, site(s) in question, and a brief description of the problem that contains pertinent information for initial issue classification.
- Maintain suitably trained technical resources familiar with the operation of the Customer's system to provide field maintenance and technical maintenance services for the system.
- Supply suitably skilled and trained on-site presence when requested.
- Validate issue resolution in a timely manner prior to close of the incident.
- Acknowledge that incidents will be addressed in accordance with Section 4.11 Priority Level Definitions and Response Time.
- Cooperate with Motorola, and perform all acts that are reasonable or necessary to enable Motorola to provide Remote Technical Support.

- In the event that Motorola agrees in writing to provide supplemental Remote Technical Support to third-party elements provided by the Customer, the Customer agrees to obtain all third-party consents or licenses required to enable Motorola to provide the service.

4.10.5 Network Hardware Repair with Advanced Replacement

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

4.10.5.1 Description of Service

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

Network Hardware Repair is also known as Infrastructure Repair.

4.10.5.2 Scope

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

4.10.5.3 Inclusions

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

Motorola Responsibilities

- Provide the Customer access to the CMSO Service Desk, operational 24/7, to request repair service.
- Provide repair return authorization numbers when requested by the Customer.
- Receive malfunctioning infrastructure components from the Customer and document its arrival, repair, and return.
- Conduct the following services for Motorola infrastructure:
 - Perform an operational check on infrastructure components to determine the nature of the problem.
 - Replace malfunctioning components.
 - Verify that Motorola infrastructure components are returned to applicable Motorola factory specifications.
 - Perform a box unit test on serviced infrastructure components.
 - Perform a system test on select infrastructure components.
- Conduct the following services for select third-party infrastructure:

- When applicable, perform pre-diagnostic and repair services to confirm infrastructure component malfunctions and prevent sending infrastructure components with No Trouble Found (NTF) to third-party vendor for repair.
- When applicable, ship malfunctioning infrastructure components to the original equipment manufacturer or third-party vendor for repair service.
- Track infrastructure components sent to the original equipment manufacturer or third-party vendor for service.
- When applicable, perform a post-test after repair by original equipment manufacturer or third-party vendor to confirm malfunctioning infrastructure components have been repaired and function properly in a Motorola system configuration.
- Reprogram repaired infrastructure components to original operating parameters based on software and firmware provided by the Customer, as required in Section 4.1.5.3: Customer Responsibilities. If the Customer's software version and configuration are not provided, shipping will be delayed. If the repair depot determines that infrastructure components are malfunctioning due to a software defect, the repair depot reserves the right to reload these components with a different but equivalent software version.
- Properly package repaired infrastructure components.
- Ship repaired infrastructure components to Customer-specified address during normal operating hours of Monday through Friday from 7:00 a.m. to 7:00 p.m. Central Standard Time (CST), excluding holidays. Infrastructure component will be sent using two-day air shipping unless the Customer requests otherwise. Motorola will pay for shipping unless the Customer requests shipments outside of the above-mentioned standard business hours or carrier programs, such as next flight out (NFO). In such cases, the Customer will be responsible for paying shipping and handling charges.

Limitations and Exclusions

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

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

- Non-standard configurations, customer-modified infrastructure, and certain third-party dropship products.
- Firmware or software upgrades.

Customer Responsibilities

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

4.10.5.4 Repair Process

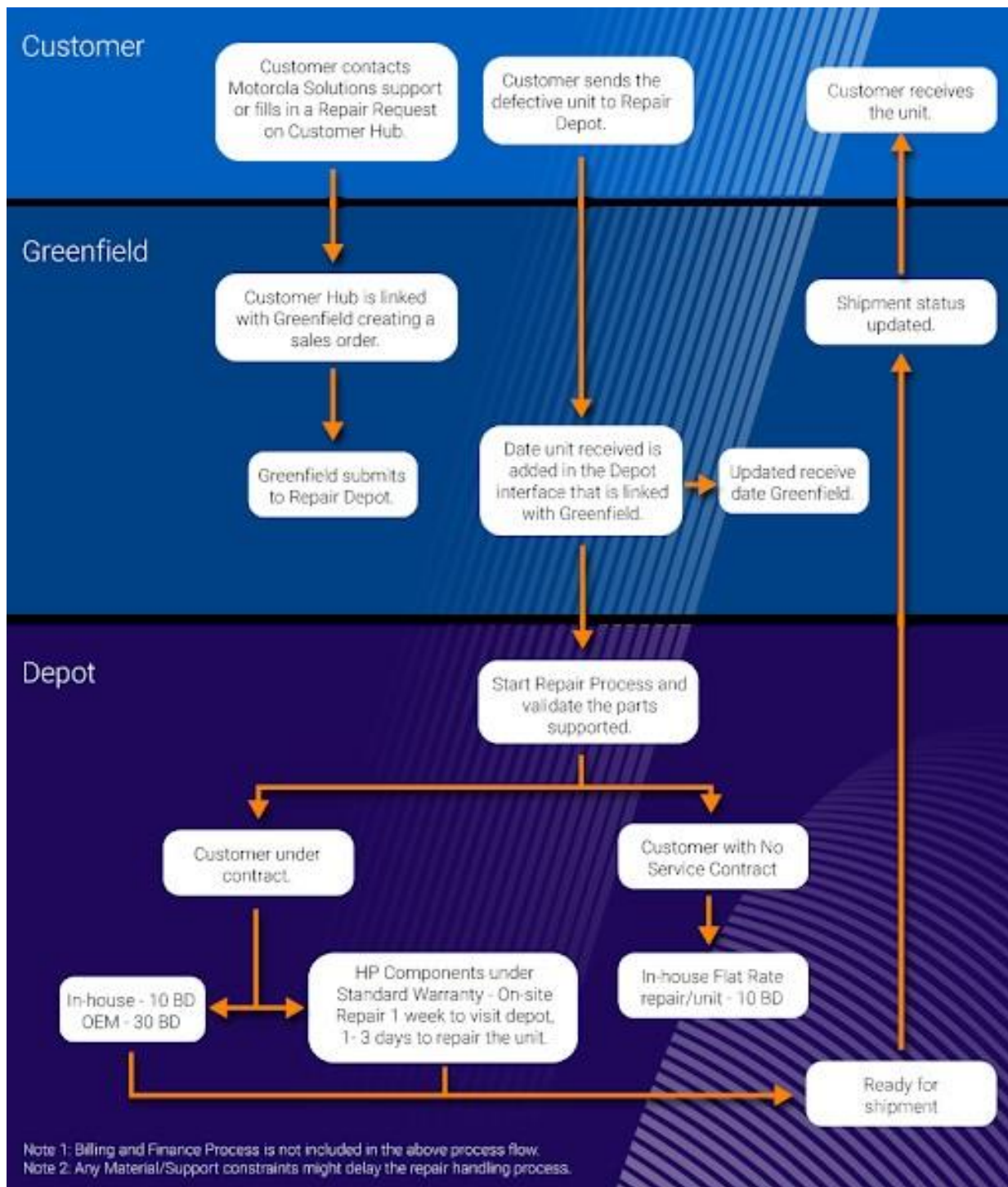


Figure 4-1: Repair Decision Process

4.10.5.5 Advanced Replacement

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

Customers who prefer to maintain their own FRU inventory may request an FRU while their unit is being repaired. Refer to Figure 4-2: Advanced Replacement Decision Process for details on the unit loan process.

Added Motorola Responsibilities for Advanced Replacement

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

Added Customer Responsibilities for Advanced Replacement

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

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

4.10.5.6 Replacement Process for Advanced Replacement

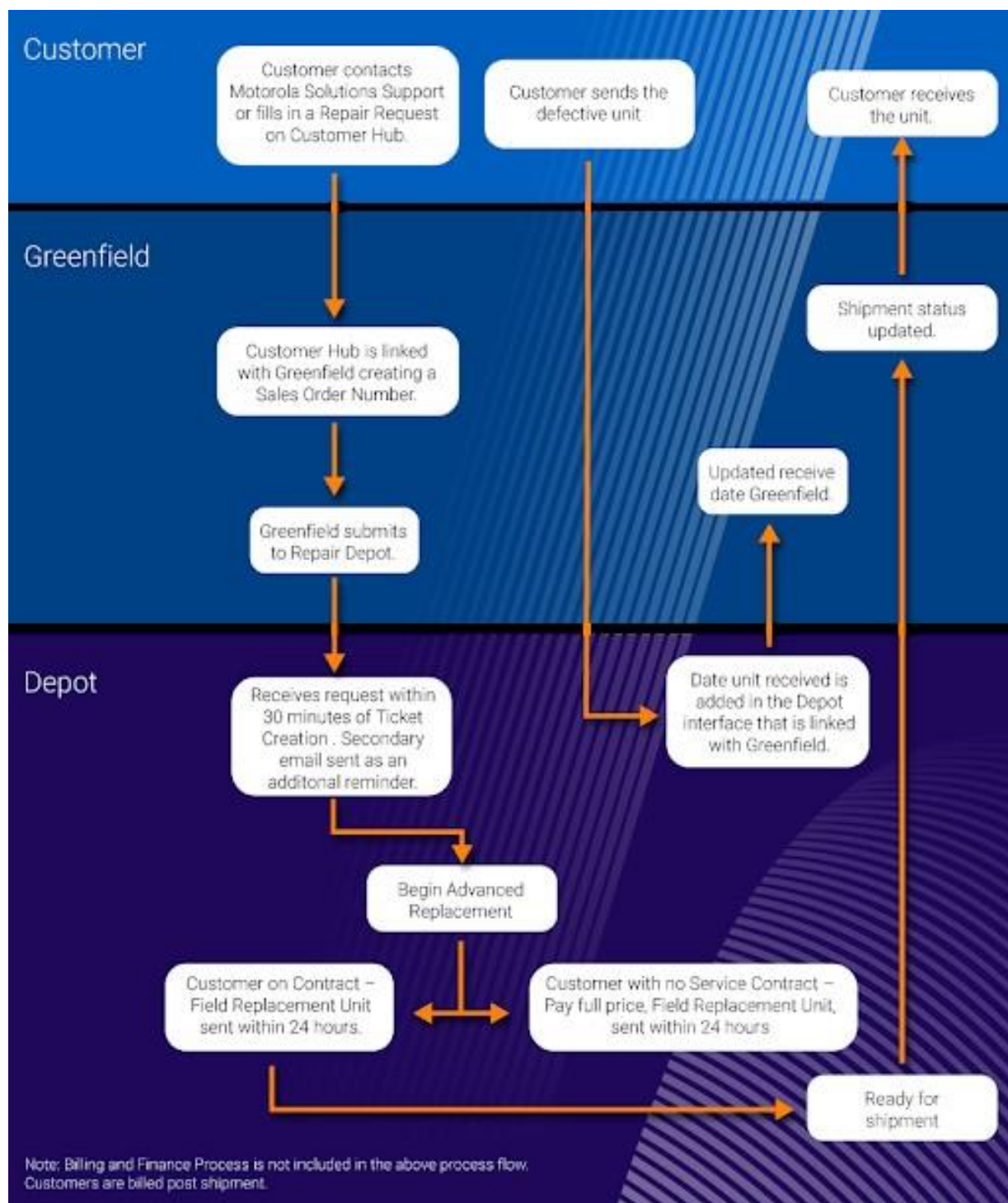


Figure 4-2: Advanced Replacement Decision Process

Table 4-7: Shipping Charges and Default Mail Service

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

Motorola shipping carrier – FedEx.

4.10.6 Security Update Service

Motorola’s ASTRO 25 Security Update Service (SUS) provides pretested security updates, minimizing cyber risk and software conflicts. These security updates contain operating system security patches and antivirus definitions that have been validated for compatibility with ASTRO 25 systems. Security update delivery is determined by the options included as part of this service. Section 4.10.6.5: Inclusions indicates if options are included as part of this service.

4.10.6.1 Description of Service

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

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

Note, the ASTRO 25 Advanced Plus Service also includes the Remote Security Update Service. See Section 4.10.7. Customer download and self-installation of security updates is only necessary for the system components that are not covered by RSUS. See **Appendix 1** for RSUS scope and exclusions.

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

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

4.10.6.2 On-Site Delivery

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

4.10.6.3 Reboot Support

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

4.10.6.4 Scope

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

Table 4-8: Update Cadence

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

4.10.6.5 Inclusions

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

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

Table 4-9: SUS Packages

Service	ASTRO 25 Core Type	Included
Security Update Service Customer Self-installed	L Core M Core Simplified Core	X
Security Update Service with Reboot Support	L Core M Core Simplified Core	NOT INCLUDED (If desired, a separate quote can be provided upon request)
Security Update Service with On-Site Delivery	L Core M Core Simplified Core	NOT INCLUDED (If desired, a separate quote can be provided upon request)

Responsibilities for downloading and installing security updates and rebooting applicable hardware are detailed in Section 4.10.6.6: Installation and Reboot Responsibilities.

Motorola Responsibilities

- On the release schedule in Section 4.10.6.4: Scope review relevant and appropriate security patches released by Original Equipment Manufacturer (OEM) vendors.
- Release tested and verified security patches to Motorola's secure website.
- Publish documentation for installation, recommended configuration changes, any identified issue(s), and remediation instructions for each security update release.
- Send notifications by email when security updates are available to download from the secure website.

Limitations and Exclusions

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

Customer Responsibilities

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

4.10.6.6 Installation and Reboot Responsibilities

Installation and Reboot responsibilities are determined by the specific SUS package being purchased.
Table 4-10: Installation and Reboot Responsibilities Matrix contains the breakdown of responsibilities.
Section 4.10.6.5: Inclusions indicates which services are included.

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

Table 4-10: Installation and Reboot Responsibilities Matrix

SUS Package	Motorola Responsibilities	Customer Responsibilities
Security Update Service Customer Self-installed		<ul style="list-style-type: none">▪ Deploy pretested files to the Customer's system as instructed in the "Read Me" text provided on Motorola's secure website.▪ When a security update requires a reboot, reboot servers and workstations after security updates are installed.

SUS Package	Motorola Responsibilities	Customer Responsibilities
OPTIONAL (not proposed) Security Update Service with On-Site Delivery	<ul style="list-style-type: none"> Dispatch a technician to deploy pretested files to the Customer's system. When a security update requires a reboot, reboot servers and workstations after security updates are installed. 	<ul style="list-style-type: none"> Acknowledge Motorola will reboot servers and workstations, and agree to timing.
OPTIONAL (not proposed) Security Update Service with Reboot Support	<ul style="list-style-type: none"> When a security update requires a reboot, dispatch a technician to reboot servers and workstations after security updates are installed. 	<ul style="list-style-type: none"> Deploy pretested files to the Customer's system as instructed in the "Read Me" text provided on Motorola's secure website.

Disclaimer

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

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

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

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

4.10.7 Remote Security Update Service

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

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

4.10.7.1 Description of Service

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

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

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

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

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

4.10.7.2 Application of Prerequisite Motorola Technical Notices (MTN)

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

4.10.7.3 Updates to System Components in the Customer Enterprise Network

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

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

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

4.10.7.4 Microsoft Windows Reboot Following Security Update Installation

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

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

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

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

4.10.7.5 Reboot Support

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

- The RSUS team will notify all listed contacts one week prior to patching to all required contacts (identified during service onboarding).
- On completion of patching, a final report is sent via email to the listed contacts.
- The notification will state that patching is complete and systems need to be rebooted.
- This process is repeated monthly.

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

4.10.7.6 Scope

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

Table 4-11: Update Cadence

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

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

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

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

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

Intrusive security updates require Customer coordination, may require hardware reboots and zone controller rolling (switching from one zone controller to the other) to fully implement. Systems with redundant zone controllers (M3) have low downtime (minutes) as the zone controllers are rolled but systems with single zone controllers will be down for longer periods. While rolling the zone controllers,

the system will operate in “site trunking” mode. The Customer will need to be aware of these operational impacts, and coordinate events with users.

4.10.7.7 Tenanted Customers Access to Antivirus Updates

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

4.10.7.8 Inclusions

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

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

Table 4-12: RSUS Options

Service	ASTRO 25 Core Type	Included
Remote Security Update Service	L Core M Core Simplified Core	YES
OPTIONAL (not proposed) Remote Security Update Service with Reboot Support	L Core M Core Simplified Core	NA

Responsibilities for rebooting applicable hardware are detailed in Section 4.10.7.9: Reboot Responsibilities.

Motorola Responsibilities

- Remotely deploy patches listed in Section 4.10.8.2: Scope on the Customer’s system. Patches will be installed on the cadence described in that section.
 - As outlined in Section 4.10.8.2: Scope, coordinate and communicate with the Customer when installing updates that will require server reboots, workstation reboots, or both.
 - Install non-intrusive updates, like antivirus definitions, as released without coordination.
- In the event that no security updates are released by the Original Equipment Manufacturers (OEM), the Final RSUS Patch Report can be reviewed by the Customer to identify where no new security updates were required.
- Coordinate RSUS activities with any other Motorola system maintenance or other engineering activities with the Customer to minimize downtime, inefficiency and operational impact.

Limitations and Exclusions

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

Customer Responsibilities

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

4.10.7.9 Reboot Responsibilities

Microsoft Windows servers and workstations often need to be rebooted before security updates take full effect and mitigate vulnerabilities. Reboot responsibilities are determined by the specific RSUS package being purchased. Table 4-13: Reboot Responsibilities Matrix contains the breakdown of responsibilities. Section 4.10.8.4: Inclusions indicates which services are included.

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

- Greater exposure to cyber security threats and vulnerabilities.

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

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

Table 4-13: Reboot Responsibilities Matrix

Remote SUS Package	Motorola Responsibilities	Customer Responsibilities
Remote Security Update Service	<ul style="list-style-type: none"> ▪ Provide a report to the Customer's main contact listing the servers or workstations which must be rebooted to ensure installed security updates become effective. 	<ul style="list-style-type: none"> ▪ When a security update requires a reboot, reboot servers and workstations after security updates are installed. ▪ When remote deployment is in progress, it may be necessary for multiple reboots to be coordinated with Motorola.
OPTIONAL (not proposed) Remote Security Update Service with Reboot Support	<ul style="list-style-type: none"> ▪ When a security update requires a reboot, dispatch a technician to reboot servers and workstations after security updates are installed. 	NA

Disclaimer

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

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

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

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

4.10.8 On-Site Infrastructure Response

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

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

4.10.8.1 Description of Service

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

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

The dispatched field service technician will travel to the Customer's location to restore the system in accordance with Section 4.10.8.5: Priority Level Definitions and Response Times.

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

4.10.8.2 Scope

On-Site Infrastructure Response is available in accordance with Section 4.10.8.5: Priority Level Definitions and Response Times. Customer's Response Time Classification is designated in the Customer Support Plan.

4.10.8.3 Geographical Availability

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

4.10.8.4 Inclusions

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

Motorola Responsibilities

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

- Close the incident upon receiving notification from the Customer or Motorola field service technician, indicating the incident is resolved.
- Notify the Customer of incident status, as defined in the CSP and Service Configuration Portal (SCP):
 - Open and closed.
 - Open, assigned to the Motorola field service technician, arrival of the field service technician on-site, delayed, or closed.
- Provide incident activity reports to the Customer, if requested.

Limitations and Exclusions

The following items are excluded from this service:

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

Customer Responsibilities

- Contact Motorola, as necessary, to request service.
- Prior to start date, provide Motorola with the following pre-defined Customer information and preferences necessary to complete CSP:
 - Incident notification preferences and procedure.
 - Repair verification preference and procedure.
 - Database and escalation procedure forms.
- Submit timely changes in any information supplied in the CSP to the CSM.
- Provide the following information when initiating a service request:
 - Assigned system ID number.
 - Problem description and site location.

- Other pertinent information requested by Motorola to open an incident.
- Provide field service technician with access to equipment.
- Supply infrastructure spare or FRU, as applicable, in order for Motorola to restore the system.
- Maintain and store software needed to restore the system in an easily accessible location.
- Maintain and store proper system backups in an easily accessible location.
- If required by repair verification preference provided by the Customer, verify with the CMSO Service Desk and dispatch that restoration is complete or system is functional.
- Cooperate with Motorola and perform reasonable or necessary acts to enable Motorola to provide these services.
- In the event that Motorola agrees in writing to provide supplemental On-Site Infrastructure Response to Customer-provided third-party elements, the Customer agrees to obtain and provide applicable third-party consents or licenses to enable Motorola to provide the service.

4.10.8.5 Priority Level Definitions and Response Times

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

Table 4-14: Standard Level Definitions and Response Times

Incident Priority	Incident Definition	On-Site Response Time
Critical P1	<p>Core: Core server or core link failure. No redundant server or link available.</p> <p>Sites/Subsites: Primary site down. Two RF sites or more than 10% of RF sites down, whichever is greater.</p> <p>Consoles: More than 40% of a site's console positions down.</p> <p>Conventional Channels: Conventional Channel Gateways (CCGW) down without redundant gateways available.</p> <p>Security Features: Security is non-functional or degraded.</p>	<p>Response provided 24/7 until service restoration.</p> <p>Field service technician arrival on-site within 4 hours of receiving dispatch notification.</p>
High P2	<p>Core: Core server or link failures. Redundant server or link available.</p> <p>Consoles: Between 20% and 40% of a site's console positions down.</p> <p>Sites/Subsites: One RF site or up to 10% of RF sites down, whichever is greater.</p> <p>Conventional Channels: Up to 50% of CCGWs down. Redundant gateways available.</p> <p>Network Elements: Site router, site switch, or GPS server down. No redundant networking element available.</p>	<p>Response provided 24/7 until service restoration.</p> <p>Field service technician arrival on-site within 4 hours of receiving dispatch notification.</p>

Incident Priority	Incident Definition	On-Site Response Time
Medium P3	Consoles: Up to 20% of a site's console positions down. Conventional Channels: Single channel down. Redundant gateway available. Network Elements: Site router/switch or GPS server down. Redundant networking element available.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 8 hours of receiving dispatch notification.
Low P4	Service Requests: Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).	Not applicable.

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

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

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

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

4.10.9 Annual Preventative Maintenance

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

4.10.9.1 Description of Service

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

4.10.9.2 Scope

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

4.10.9.3 Inclusions

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

Table 4-17: Preventive Maintenance Level

Service Level	Included
Level 1 Preventive Maintenance	X

Motorola Responsibilities

- Notify the Customer of any planned system downtime needed to perform this service.
- Maintain communication with the Customer as needed until completion of the Annual Preventive Maintenance.
- Determine, in its sole discretion, when an incident requires more than the Annual Preventive Maintenance services described in this SOW, and notify the Customer of an alternative course of action.
- Provide the Customer with a report in Customer Hub, or as otherwise agreed in the CSP, comparing system performance with expected parameters, along with any recommended actions. Time allotment for report completion is to be mutually agreed.
- Provide trained and qualified personnel with proper security clearance required to complete Annual Preventive Maintenance services.
- Field service technician will perform the following on-site:
- Perform the tasks defined in Section 4.10.9.4: Preventative Maintenance Tasks.
 - Perform the procedures defined in Section **Error! Reference source not found.: Error! Reference source not found.** for each site type on the system.
 - Provide diagnostic and test equipment necessary to perform the Preventive Maintenance service.
 - As applicable, use the Method of Procedure (MOP) defined for each task.

Limitations and Exclusions

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

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

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

Customer Responsibilities

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

4.10.9.4 Preventative Maintenance Tasks

The Preventive Maintenance service includes the tasks listed in this section. Tasks will be performed based on the level of service noted in Section 4.10.9.3: Inclusions.

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

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

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

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

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

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

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

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

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

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

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

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

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

4.10.10 System Upgrade Agreement (SUA)

4.10.10.1 Overview

Utilizing the ASTRO System Upgrade Agreement (SUA) service, City of Gahanna (Customer) is able to take advantage of new functionality and security features while extending the operational life of the system.

Motorola continues to make advancements in on-premises and cloud technologies to bring value to our customers. Cloud technologies enable the delivery of additional functionality through frequent updates ensuring the latest in ASTRO is available at all times.

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

The Customer is required to keep the system within a standard support period as described in Motorola's [Software Support Policy \(SwSP\)](#).

4.10.10.2 Scope

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 (System Upgrade) in each eligible System Upgrade window over the term of this agreement. The term of the agreement is listed in Table 4-18: SUA Terms. The eligible System Upgrade windows and their duration are illustrated in Table 4-19: Eligible Upgrade Window.

With the addition of the cloud services, Motorola will provide continuous updates to the cloud core to enable the delivery of additional functionality. Cloud updates will be more frequent than the ASTRO System Upgrades and will occur outside the defined eligible System Upgrade windows in Table 4-19: Eligible Upgrade Window. Motorola may, at its sole discretion, automatically apply the cloud updates as they become available.

If needed to perform the System Upgrade, Motorola will provide updated and/or replacement hardware for covered infrastructure components. System Upgrades, when executed, will provide an equivalent level of functionality as that originally purchased and deployed by the Customer. At Motorola's option, new system releases may introduce new features or enhancements that Motorola may offer separately for purchase.

NOTE: The SUA service Eligible Upgrade Window timing will be determined based upon the final outyear purchase by the Customer.

Table 4-18: SUA Terms

Duration	Optional 4 Years (see Outyear pricing in Pricing Section of this proposal)
-----------------	--

Table 4-19: Eligible Upgrade Window

First Eligible Upgrade Window	Second Eligible Upgrade Window
Duration: 2 years (optional)	Duration: 2 years (optional)
TBD	TBD

The methodology for executing each System Upgrade is described in Section 4.10.10.12. ASTRO SUA pricing is based on the system configuration outlined in Appendix B: System Pricing Configuration. This configuration is to be reviewed annually from the contract effective date. Any change in system configuration may require an ASTRO SUA price adjustment.

The price quoted for ASTRO SUA requires the Customer to choose a certified system upgrade path in Appendix A: ASTRO System Release Upgrade Paths. Should the Customer elect an upgrade path other than one listed in Appendix A: ASTRO System Release Upgrade Paths, the Customer agrees that additional fees may be incurred to complete the implementation of the system upgrade. In this case, Motorola will provide a price quotation for any additional materials and services necessary.

4.10.10.3 Inclusions

Refer to Table C-4: SUA Coverage Table for more detailed information on the SUA inclusions referenced in this section.

4.10.10.4 System Upgrades

System Upgrade coverage includes the products outlined in Appendix B: System Pricing Configuration and does not cover all products. The ASTRO SUA applies only to System Upgrades within the ASTRO platform and entitles the Customer to eligible past software versions for downgrading product software to a compatible release version. Past versions from within the Standard Support Period will be available.

4.10.10.5 Subscriber Radio Software

The ASTRO SUA makes available the subscriber radio software releases that are shipping from the factory during the coverage period. Please refer to Section 4.10.10.12: General Statement of Work for System Upgrades.

4.10.10.6 Limitations and Exclusions

The parties acknowledge and agree that the ASTRO 25 SUA does not cover the products and services detailed in this section.

Table 4-20: SUA Limitations and Exclusions

Excluded Products and Services	Examples, but not limited to
Purchased directly from a third party	NICE, Genesis, Verint
Residing outside of the ASTRO 25 network	CAD, E911, Avtec Consoles
Not certified on ASTRO 25 systems	Laptops, PCs, Eventide loggers
Backhaul Network	MPLS, Microwave, Multiplexers
Two-Way Subscriber Radios	APX, MCD 5000, Programming, Installation
Consumed in normal operation	Monitors, microphones, keyboards, speakers
RFDS and Transmission Mediums	Antennas, Transmission Line, Combiners
Customer provided cloud connectivity	LTE, Internet
Maintenance Services of Any Kind	Infrastructure Repair, Tech Support, Dispatch
Security Services	Security Update Service (SUS), Remote SUS

4.10.10.7 Platform Migrations

Platform Migrations are the replacement of a product with the next generation of that product that is not within the same product family. This can be defined as a new technology that is based on a new hardware configuration and/or a new underlying software. Any upgrades 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 in this document, Platform Migrations such as, but not limited to, stations, comparators, site controllers, consoles, backhaul, and network changes are not included.

4.10.10.8 Non-Standard Configurations

Systems that have non-standard configurations that have not been certified by Motorola Systems Integration Testing are specifically excluded from the ASTRO SUA unless otherwise included in this SOW. Customer acknowledges that if the system has a Special Product Feature it may be overwritten by the software upgrade. Restoration of that feature is not included in the coverage of this SOW.

4.10.10.9 System Expansions and New Features

Any upgrades to hardware versions, replacement hardware, and/or implementation services that are not directly required to support the certified System Upgrade are not included unless otherwise agreed to in writing by Motorola. This exclusion applies to, but is not limited to, system expansions and new features.

4.10.10.10 Cloud Technology

Support for Customer-provided connectivity to the cloud platform is not covered under this agreement. Future cloud, IT, and security related adoption is an evolving technological area and laws, regulations, and standards relating to ASTRO SUA may change. Any changes to ASTRO SUA required to achieve future regulatory or Customer specific compliance requirements are not included.

4.10.10.11 Subscriber Radio Software

Applying software updates to subscriber radios is the Customer's responsibility and is not included in SUA coverage. Subscriber radios must be at a software release compatible with the Customer's ASTRO system configuration. Motorola will make reasonable efforts to notify the Customer if there is an incompatibility.

4.10.10.12 General Statement of Work for System Upgrades

4.10.10.12.1 Upgrade Planning and Preparation

All items listed in this section are to be completed at least 6 months prior to a scheduled upgrade.

Motorola Responsibilities

- Obtain and review infrastructure system audit data as needed.
- Identify the backlog accumulation of security patches and antivirus upgrades needed to implement a system release. If applicable, provide a quote for the necessary labor, security patches, and antivirus upgrades.
- If applicable, identify additional system hardware needed to implement a system release.
- Identify Customer provided hardware that is not covered under this agreement, or where the Customer will be responsible for implementing the system release upgrade software.
- Identify the equipment requirements and the installation plan.
- Advise the Customer of probable impact to system users during the cloud update and the actual field upgrade implementation.
- If applicable, advise the Customer on the network connection specifications necessary to perform the System Upgrade.

- Where necessary to maintain existing functionality and capabilities, deploy and configure any additional telecommunications equipment necessary for connectivity to the cloud-based technologies.
- Assign program management support required to perform the certified System Upgrade. Prepare an overall System Upgrade schedule identifying key tasks and personnel resources required from Motorola and Customer for each task and phase of the System Upgrade. Conduct a review of this schedule and obtain mutual agreement of the same.
- Assign installation and engineering labor required to perform the certified System Upgrade.
- Provide access to cloud training videos, frequently asked questions, and help guide.
- 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 System 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.

Customer Responsibilities

- Contact Motorola to schedule and engage the appropriate Motorola resources for a system upgrade. Contact Motorola to schedule a System Upgrade and provide necessary information requested by Motorola to execute the System Upgrade. Review System Upgrade schedule and reach mutual agreement of the same.
- Identify hardware not purchased through Motorola that will require the system release upgrade software.
- Purchase the security patches, antivirus upgrades and the labor necessary to address any security upgrades backlog accumulation identified in Section 4.10.6.5: Motorola Responsibilities, if applicable. Unless otherwise agreed in writing between Motorola and Customer, the installation and implementation of accumulated backlog security patches and network updates is the responsibility of the Customer.
- If applicable, provide network connectivity at the zone core site(s) for Motorola to use to download and pre-position the software that is to be installed at the zone core site(s) and pushed to remote sites from there. Motorola will provide the network connection specifications, as listed in Section 4.10.2.4 Connectivity. Network connectivity must be provided at least 12 weeks prior to the scheduled System Upgrade. In the event access to a network connection is unavailable, the Customer may be billed additional costs to execute the System Upgrade.
- Assist in site walks of the system during the system audit when necessary.
- Provide a list of any FRUs and/or spare hardware to be included in the System Upgrade when applicable. Upon reasonable request by Motorola, Customer will provide a complete serial and model number list of the equipment. The inventory count of Customer FRUs and/or spare hardware to be included as of the start of the SUA is included in Appendix B: System Pricing Configuration.
- Acknowledge that new and optional system release features or system expansions, and their required implementation labor, are not within the scope of the SUA. The Customer may purchase these under a separate agreement.
- Maintain an internet connection between the on-premise radio solution and the cloud platform, unless provided by Motorola under separate Agreement.

- Identify any Customer specific standard or requirements that may be implicated by the planned upgrade(s), including heightened cloud, IT, or information security related standards or requirements, such as those that may apply to U.S. Federal Customer or other government Customer standards. Motorola makes no representations as to the compliance of ASTRO SUA with any Customer specific standards, requirements, specifications, or terms, except to the extent expressly specified.
- Participate in release impact training at least 12 weeks prior to the scheduled System 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.

4.10.10.13 System Readiness Checkpoint

All items listed in this section are to be completed at least 30 days prior to a scheduled upgrade.

Motorola Responsibilities

- Perform appropriate system backups.
- Work with the Customer to validate that all system maintenance is current.
- Work with the Customer to validate that all available security patches and antivirus upgrades have been upgraded on the Customer's system.
 - Motorola reserves the right to charge the Customer for the security patches, antivirus updates and the labor necessary to address any security updates backlog accumulation, in the event that these are not completed by the Customer at the System Readiness Checkpoint.

Customer Responsibilities

- Validate that system maintenance is current.
- Validate that all available security patches and antivirus upgrades to the Customer's system have been completed or contract Motorola to complete in time for the System Readiness Checkpoint.

4.10.10.14 System Upgrade

Motorola Responsibilities

- Perform system infrastructure upgrade for the system elements outlined in this SOW.

Customer Responsibilities

- Inform system users of software upgrade plans and scheduled system downtime.
- Cooperate with Motorola and perform all acts that are reasonable or necessary to enable Motorola to provide software upgrade services.

4.10.10.15 Upgrade Completion

Motorola Responsibilities

- Validate all certified system upgrade deliverables are complete as contractually required.
- Confirm with Customer that the cloud is available for beneficial use.

Customer Responsibilities

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

4.10.10.16 Special Provisions

The migration of capabilities from ASTRO 25 on-premises infrastructure to the cloud is not considered to be a platform migration and is therefore included in the deliverable of the SUA agreement. Technologies based on cloud architecture will be a part of the Motorola roadmap and may be subject to additional cloud terms and conditions.

The SUA does not extend to customer-provided software and hardware. Motorola makes no warrants or commitments about adapting our standard system releases to accommodate customer implemented equipment. If during the course of an upgrade, it is determined that customer provided software and/or hardware does not function properly, Motorola will notify the customer of the limitations. The customer owns any costs and liabilities associated with making the customer provided software and/or hardware work with the standard Motorola system release. This includes, but is not limited to, Motorola costs for the deployment of resources to implement the upgrade once the limitations have been resolved by the customer.

Any Motorola software, including any system releases, is licensed to Customer solely in accordance with the applicable Motorola Software License Agreement. Any non-Motorola Software is licensed to Customer in accordance with the standard license, terms, and restrictions of the copyright owner unless the copyright owner has granted to Motorola the right to sublicense the Non-Motorola Software pursuant to the Software License Agreement, in which case it applies and the copyright owner will have all of Licensor's rights and protections under the Software License Agreement. Motorola makes no representations or warranties of any kind regarding non-Motorola Software. Non-Motorola Software may include Open-Source Software.

ASTRO 25 SUA coverage and the parties' responsibilities described in this SOW 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 program. In either case, Motorola will refund to Customer any prepaid fees for ASTRO 25 SUA applicable to the terminated period.

If the 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 Upgrade Operations Team.

The ASTRO 25 SUA annualized price is based on the fulfillment of the system release upgrade in each eligible upgrade window. If the Customer terminates, except if Motorola is the defaulting party, the Customer will be required to pay for the balance of payments owed in that eligible upgrade window if a system release upgrade has been taken prior to the point of termination.

Appendix A: ASTRO 25 System Release Upgrade Paths

The upgrade paths for standard ASTRO system releases are listed in Table A-1: Certified Standard ASTRO 25 System Release Upgrade Paths.

Table A-1: Certified Standard ASTRO 25 System Release Upgrade Paths

ASTRO 25 System Release	Certified Upgrade Paths
Pre-7.17.X	Upgrade to Current Shipping Release
A7.17.X	A2020.1
A7.18	A2021.1
A2019.2	A2021.1
A2020.1	A2022.1
A2021.1	A2022.1

The upgrade paths for high security ASTRO system releases for federal deployments are described in Table A-2: Certified High Security ASTRO 25 System Release Upgrade Paths.

Table A-2: Certified High Security ASTRO 25 System Release Upgrade Paths

ASTRO 25 High Security System Release	Certified Upgrade Paths
A7.17.X	A2020.HS
A2020.HS	A2022.HS

The release taxonomy for the ASTRO 25 7.x platform is expressed in the form “ASTRO 25 7.x release 20YY.Z”. In this taxonomy, YY represents the year of the release, and Z represents the release count for that release year.

A20XX.HS enhances the ASTRO 25 System release with support for Public key infrastructure (PKI) Common Access Card/Personal Identity Verification (CAC/PIV) and with Cyber Security Baseline Assurance.

- The most current system release upgrade paths can be found in the most recent Lifecycle Services bulletin.
- The information contained herein is provided for information purposes only and is intended only to outline Motorola’s presently anticipated general technology direction. The information in the roadmap is not a commitment or an obligation to deliver any product, product feature or software functionality and Motorola reserves the right to make changes to the content and timing of any product, product feature, or software release.

Appendix B: System Pricing Configuration

This configuration is to be reviewed annually from the contract effective date. Any change in system configuration may require an ASTRO 25 SUA price adjustment.

Table B-3: System Configuration

System Configuration	
Core Configurations	
Cloud based Core	0
On-premises Main Site	0
On-premises Backup Site	0

System Configuration	
System Level Features	
Standalone servers (Critical Connect / Smart Connect)	0
MOSCAD NFM RTU (typically 1 per site location)	0
Network Management Clients	0
IMW Servers	0
Telephone Interconnect	0
Security Configurations	
AERSS Sensors	1
Firewalls	1
KMF Servers	0
KMF Clients	0
RF Site Configurations	
Virtual Prime Sites	0
IP Simulcast Prime Sites (include co-located/redundant)	0
RF Sites (include Simulcast sub-sites, ASR sites, HPD sites)	0
GTR 8000 Base Stations	0
Dispatch Site Configurations	
Dispatch Site Locations	0
MCC 7500 Dispatch Consoles	0
AIS	1
CCGWs	2
MC EDGE Aux I/O	1
AXS Console Dispatch Site Locations	1
AXS Console PDH (Command Central Hub)	7
AXS Servers	0
Third Party Elements	
NICE Logging recorders (IP, Telephony, or Analog) Purchased through Motorola	0
MACH Alert FSA Purchased through Motorola	0
Genesis Applications Purchased through Motorola	0

Appendix C: SUA Coverage Table

This appendix includes a breakdown of coverage under the SUA. System Upgrade coverage includes software and hardware coverage for equipment originally provided by Motorola. A “board-level replacement” is defined as any Field Replaceable Unit (FRU).

Table C-4: SUA Coverage Table

ASTRO Certified Solution		System Upgrade		
Equipment Provided by Motorola		Software	Hardware Full Product	Hardware Board-Level
Servers		✓	✓	
Workstations		✓	✓	
Firewalls		✓	✓	
Routers		✓	✓	
LAN Switches		✓	✓	
CirrusNode		✓	✓	
MCC 7500 Voice Processing Module		✓		✓
MCC 7500E Dispatch AIM		✓	✓	
MCC 7500E Dispatch (CommandCentral Hub)		✓	✓	
AXS PDH Client (CommandCentral Hub)		✓	✓	
SDM 3000 Aux I/O		✓	✓	
MC Edge Aux I/O		✓	✓	
GTR 8000 Base Stations		✓		✓
GCP 8000 Site Controllers		✓		✓
DSC 8000 Site Controllers		✓	✓	
GCM 8000 Comparators		✓		✓
Motorola logging interface equipment		✓	✓	
PBX switches for telephone interconnect		✓	✓	
SDM 3000 RTU		✓		✓
Conventional Channel Gateway (CCGW)		✓	✓	
NICE IP logging solutions (if software, hardware and lifecycle purchased from Motorola)		✓	✓	
MACH Alert FSA (if software, hardware and lifecycle purchased from Motorola)		✓	✓	
Genesis Applications (if software, hardware and lifecycle purchased from Motorola)		✓	✓	

4.11 Priority Level Definitions and Response Time

Table 4-21: Priority Level Definitions and Response Time describes the criteria Motorola uses to prioritize incidents and service requests, and lists the response times for those priority levels.

Table 4-21: Priority Level Definitions and Response Time

Incident Priority	Incident Definition	Initial Response Time	On-Site Response Time
Critical P1	<ul style="list-style-type: none"> ▪ Core: Core server or core link failure. No redundant server or link available. ▪ Sites/Subsites: Primary site down. Two RF sites or more than 10% of RF sites down, whichever is greater. ▪ Consoles: More than 40% of a site's console positions down. ▪ Conventional Channels: Conventional Channel Gateways (CCGW) down without redundant gateways available. ▪ Security Features: Security is non-functional or degraded. ▪ Alarm Events: Door, motion, intrusion, power failure, or environmental alarms triggered. 	Response provided 24/7 until service restoration. Technical resource will acknowledge incident and respond within 30 minutes of CMSO logging incident.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
High P2	<ul style="list-style-type: none"> ▪ Core: Core server or link failures. Redundant server or link available. ▪ Consoles: Between 20% and 40% of a site's console positions down. ▪ Sites/Subsites: One RF site or up to 10% of RF sites down, whichever is greater. ▪ Conventional Channels: Up to 50% of CCGWs down. Redundant gateways available. ▪ Network Elements: Site router, site switch, or GPS server down. No redundant networking element available. 	Response provided 24/7 until service restoration. Technical resource will acknowledge incident and respond within 1 hour of CMSO logging incident.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.

Incident Priority	Incident Definition	Initial Response Time	On-Site Response Time
Medium P3	<ul style="list-style-type: none"> ▪ Consoles: Up to 20% of a site's console positions down. ▪ Conventional Channels: Single channel down. Redundant gateway available. ▪ Network Elements: Site router/switch or GPS server down. Redundant networking element available. 	Response provided during normal business hours until service restoration. Technical resource will acknowledge incident and respond within 4 hours of CMSO logging incident.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 8 hours of receiving dispatch notification.
Low P4	<ul style="list-style-type: none"> ▪ Service Requests: Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work). 	Response provided during normal business hours. Motorola will acknowledge and respond within 1 Business Day.	Not applicable.

4.12 Appendix 1 ASTRO 25 Remote Security Update Coverage

4.12.1 RSUS Coverage

The following table defines which components are covered by the Remote SUS service. The ASTRO 25® Point Service Software Support Policy applies. Security Update Service (SUS) and Remote Security Update Service (RSUS) support only systems that are within the Standard Software Support Period (up to 4 years after general release). Support is dependent on connectivity to the (RNI) Radio Network Infrastructure.

Table 4-22: RSUS Covered Components

SOFTWARE	UPDATE RELEASE CADENCE	PRODUCTS * DEPENDS ON DEVICE NETWORK LOCATION IN RNI OR CONNECTIVITY SETTINGS *
Antivirus Definition Files	Weekly	<ul style="list-style-type: none"> Based on automated (CSMS) Core Security Management Server configurations
Microsoft Windows	Monthly	<ul style="list-style-type: none"> (AMS) Advanced Messaging Server (AuC) Authentication Center Client (AuC) Authentication Center Server (CSMS) Core Security Management Server (DC) Domain Controller (IPPBX) (ETI) Enhanced Telephone Interconnect (KMF) Key Management Framework Client (KMF) Key Management Framework Server (MCC) Master Control Console 5500 (MCC) Master Control Console 7100 (MCC) Master Control Console 7500 / (AIS) Archiving Interface Server (MCC) Master Control Console 7500 E (MCC) Master Control Consoles 7500 E (NM) Network Management Client (OPSOC) On-Prem Security Operations Center (RM) Radio Management Client (RM) Radio Management Server MACH Alert (FSA) Fire Station Alerting Marvlis AVL Desktop Monitor Marvlis Server NICE (AIS) Archiving Interface Server NICE Backup Server NICE IP Radio Logger NICE Replay Workstation Proxy 7000 Transcoder Verint Logging Recorder Server Verint Workstation
Microsoft Windows SQL Server	Quarterly	<ul style="list-style-type: none"> (CSMS) Core Security Management Server

SOFTWARE	UPDATE RELEASE CADENCE	PRODUCTS * DEPENDS ON DEVICE NETWORK LOCATION IN RNI OR CONNECTIVITY SETTINGS *
Red Hat Linux (RHEL)	Quarterly	<ul style="list-style-type: none"> • (ATR) Air Traffic Router • (BAR) Backup and Restore Server • (IPCAP) IP Packet Capture • (ISGW) Intersystem Gateway • (LM) License Manager • (LMP) LMP Multicast Proxy • (NTP) Network Time Protocol • (PDG) Packet Data Gateway • (SSS) System Statistical Service • (Syslog) Syslog Service • (UCS) User Configuration Server • (UEM) Unified Event Manager • (UNC) Unified Network Configurator • (ZC) Zone Controller • (ZDS) Zone Database Service • (ZSS) Zone Statistical Server
VMWare ESXi Hypervisor	Quarterly	<ul style="list-style-type: none"> • (VMS) Virtual Management Server
VMWare vCenter	Quarterly	<ul style="list-style-type: none"> • (VCLS) vSphere Cluster Services
McAfee/Trellix Patch(es)	Quarterly	<ul style="list-style-type: none"> • (CSMS) Core Security Management Server
Dot Hill DAS Firmware	Quarterly	<ul style="list-style-type: none"> • 4524 • 4525
HP SPP Firmware	Quarterly	<ul style="list-style-type: none"> • HP Generation 9 • HP Generation 10

4.13 Exclusions

The following system components are not covered by RSUS but are covered by the SUS service. If you require assistance to deploy these updates, please contact your CSM to arrange Onsite SUS services.

Table 4-23: Excluded Components

Software	Products
Product Lines	<ul style="list-style-type: none"> • (IMW) Intelligent MiddleWare Server • WAVE Radio Gateway • WAVE Tactical • (PA) Personnel Accountability • (CEN) Customer Enterprise Network Located Loggers (including Telephony)
Antivirus Definition Files	<ul style="list-style-type: none"> • Stand Alone Deployed Products
Microsoft Windows	<ul style="list-style-type: none"> • (CAM) Console Alias Manager Server • Genesis Genwatch3 • Genesisworld Performance Management Solutions Client
Microsoft Windows SQL Server	<ul style="list-style-type: none"> • NICE IP Logging Recorder
QNAP	<ul style="list-style-type: none"> • TS453A • TS453Be • TS453D • TS-464
PostgreSQL	<ul style="list-style-type: none"> • (KMF) Key Management Framework Server
McAfee/Trellix Patch(es)	<ul style="list-style-type: none"> • Stand Alone Deployed Products

There may be components not included in the tables above. These components are not covered.

Section 5

Training Plan

5.1 Overview

Motorola Solutions understands that successful implementation and use of your communications system depends on effective training. We have developed a training proposal for City of Gahanna to ensure a comprehensive understanding of your proposed system and all user equipment. We are leveraging over 90 years of training experience working with customers just like you to provide recommendations for your consideration. The training proposal detailed in the following pages incorporates customer feedback coupled with a best practices systematic approach to produce effective course delivery and content.

Motorola Solutions' commitment is to provide unsurpassed services that ensure the equipment operates efficiently for the life of the system. To do so, we directly train your personnel to utilize the system to its maximum potential.

The training offering ensures your personnel will gain in-depth understanding of the power of the proposed new system through education and proficient daily use. Our high-quality training focuses on student needs. The training is complemented by detailed documentation and available continuing education programs.

We will collaborate to develop a final customized training plan that fits your needs. Our goal is to ensure system administrators, technicians and end-users are skilled in using your new system.



5.2 Training Approach

Our training solutions deliver a combination of online training and field-based instructor-led training in classrooms at Customer designated locations using operational equipment. Motorola Solutions will employ knowledgeable and experienced instructors to deliver well-designed courseware and integrated lab activities.

Training is based upon several key criteria:

- Course design is driven by an analysis of student needs. It focuses on specific application rather than theory.
- Learning objectives are based upon what students need to accomplish on the job.
- Hands-on lab opportunities using specific job aids are incorporated to maximize learning and retention.

Our instructors bring invaluable experience and knowledge of customer communication solutions into their training approach. This gives them better insight and understanding into the practical aspects of

the manager, technician and end-user job functions. Each instructor has the proven ability to communicate with a novice as well as expert personnel.

5.3 Proposed Courses

Motorola Solutions has identified the following course(s) that are necessary to achieve the training goals. Class delivery for instructor-led courses in the field will be tailored for your system and features.

Specifically, our proposed training plan addresses the following categories as identified in your request for proposal:

- Console Operators and Dispatch Supervisors

It is recommended that participants bring their laptop computers for all system administrator and technician classes.

5.4 Seven Position Training

5.4.1 Console Operator and Supervisor Training Plan

Course Title	Target Audience	Sessions	Duration	Location	Date	Participants
AXS Console Operator and Admin Utilizing the Interactive End User Tool Kit 7 training consoles (Instructor-led)	Dispatch Supervisors	1 (8-hour session)	1 day	US	Prior to cutover	7
AXS Console Operator 7 training consoles (Instructor-led) Please Note: One (1) extra instructor day and one (1) extra Session have been added to cover 3 rd shift training.	Dispatch Operators	5 (4-hour sessions)	3 days	US	Prior to cutover	35 (5 Per Session)

5.5 Course Outlines

Course outlines for the AXS Dispatch operator and AXS supervisor can be found on the following pages.

5.5.1 AXS Operator

Duration

- Normally four (4) hours.
- Specially tailored two (2)-hour session.

Delivery Method

- Instructor-led.

Target Audience

- Dispatch Console Operators, Supervisors, System Administrators, and Support Personnel.

Course Synopsis

This course provides participants with an introduction to the dispatch console, its basic operation and tailored job aids which will be available for assistance in operation. Through facilitation and hands-on activities, the user learns how to perform common tasks associated with the console operation.

Course Objectives

- Perform basic operational tasks of the dispatch console.
- Utilize the provided job aids to perform specific tasks associated with the console.
- Understand a high-level view of the system configuration.
- High-level overview of the customer system configuration.
- General console operation.
- Proper operating procedures for specific customer features.

Recommended Prerequisites

- None.

Key Topics

- Overview.
- Communicating with Radios.
- Advanced Signaling Features.
- Resource Groups.
- Working with Configurations.
- Working with Aux IOs.
- Troubleshooting.

5.5.2 AXS Supervisor

Duration

- 4 hours Operator, plus
- 4 hours Admin.

Delivery Method

- Instructor-led.

Target Audience

- Dispatch Supervisors, System Administrators.

Admin Course Synopsis

This course provides participants with the knowledge and skills to manage and utilize the AXS console administrator functions. Through facilitation and hands-on activities, the participant learns how to customize the console screens.

Course Objectives

- Understand the menu items and tool bar icons.
- Edit folders, multiselect/patch groups, auxiliary input output groups, windows and toolbars.
- Add/delete folders.

Recommended Prerequisites

- None.

Key Topics

- Introduction.
- Configurations.
- Folders and Resource Setup.
- Customizing Folders.
- Auto Starting the AXS Dispatch Console.
- Editing Preferences.
- Configuring the Toolbar.
- Setting Up Aux IOs.
- Resource Groups

Section 6

Pricing Summary

6.1 AXS Dispatch Site

EQUIPMENT AND SERVICES SUMMARY		Price
New AXS Dispatch site with (7) Console Positions, Implementation Services and Year 1 Warranty included.		\$822,435
TOTAL SYSTEM SALE PRICE with purchase by June 9, 2025		\$822,435
Advance Plus Lifecycle Services (Total Years 2-5, annuals below)		
TOTAL SYSTEM SALE PRICE & YEARS 2-5 with purchase by June 9, 2025		\$1,258,709
LIFECYCLE SERVICES - Optional		
Advanced Plus Lifecycle Services - Year 2		\$103,417
Advanced Plus Lifecycle Services - Year 3		\$107,085
Advanced Plus Lifecycle Services - Year 4		\$110,902
Advanced Plus Lifecycle Services – Year 5		\$114,870

6.2 Pricing Terms and Conditions

- Prices quoted per Ohio State Term Schedule #573077-0.
- See attached Motorola Solutions Customer Agreement (MCA) Exhibit A for payment terms.
- Pricing valid through June 9, 2025.
- Pricing for optional items is only valid at time of original offer/purchase and will be subject to pricing change if purchased at a later date.

6.3 Maintenance and Lifecycle Services

NOTE: Lifecycle Services proposed above are for maintenance and system upgrades after year 1. These services can be purchased with this proposal or as a separate purchase. As an Add On to Ohio MARCS all add-ons are required to align with the regular MARCS System Upgrade schedule through 2039 and must include security monitoring and security update services. The annual pricing defined above includes these MARCS required services.

Section 7

Contractual Documentation

Motorola's Motorola Solutions Customer Agreement is attached in the pages below.

Motorola Solutions Customer Agreement

This Motorola Solutions Customer Agreement (the “**MCA**”) is entered into between Motorola Solutions, Inc., with offices at 500 W. Monroe Street, Suite 4400, Chicago, IL 60661 (“**Motorola**”) and the entity set forth in the signature block below (“**Customer**”). Motorola and Customer will each be referred to herein as a “**Party**” and collectively as the “**Parties**”. This Agreement (as defined below) is effective as of the date of the last signature (the “**Effective Date**”).

Section 1. Agreement.

1.1. Scope; Agreement Documents. This MCA governs Customer’s purchase of Products and Services (as each are defined below) from Motorola. Additional terms and conditions applicable to specific Products and Services are set forth in one or more Motorola prepared or agreed upon addenda attached to this MCA (each an “**Addendum**”, and collectively the “**Addenda**”). This MCA, the Exhibits, Addenda, and Motorola-provided Proposal collectively form the Parties’ “**Agreement**”.

1.2. Attachments. The Exhibits listed below will be attached hereto and incorporated into and made a part of this Agreement:

- Exhibit A “Payment” (Communications System purchase only)
- Exhibit B Motorola Proposal dated _____
- Exhibit C “System Acceptance Certificate” (Communications System only)

1.3. Order of Precedence. In interpreting this Agreement and resolving any ambiguities: 1) the main body of this Agreement takes precedence over the exhibits (unless otherwise specified in an exhibit), and any inconsistency between Exhibits A through C will be resolved in their listed order, and 2) Each Addendum will control with respect to conflicting terms in the Agreement, but only as applicable to the Products and Services described in such Addendum.

Section 2. Definitions.

“**Authorized Users**” means Customer’s employees, full-time contractors engaged for the purpose of supporting the Products and Services that are not competitors of Motorola, and the entities (if any) specified in a Proposal or otherwise approved by Motorola in writing (email from an authorized Motorola signatory accepted), which may include affiliates or other Customer agencies.

“**Change Order**” means a written amendment to this Agreement after the effective date that alters the work, the contract sum, the contract time, or other change mutually decided between the Parties.

“**Communications System**” is a solution that includes at least one radio Product, whether devices, software, or infrastructure, and requires Integration Services to deploy such radio Product at a Customer Site or onto any Customer-Provided Equipment or Equipment provided to Customer.

“**Contract Price**” means the price for the Communications System and implementation Services, excluding applicable sales or similar taxes and freight charges. Further, unless otherwise stated in Exhibit A “Payment” or the pricing pages of the Proposal, recurring fees for maintenance, SUA, or Subscription Software are included in the Contract Price.

“**Confidential Information**” means any and all non-public information provided by one Party to the other that is disclosed under this Agreement in oral, written, graphic, machine recognizable, or sample form, being clearly designated, labeled or marked as confidential or its equivalent or that a reasonable business person would consider non-public and confidential by its nature. With respect to Motorola,

Confidential Information will also include Products and Services, and Documentation, as well as any other information relating to the Products and Services.

“Customer Contact Data” has the meaning given to it in the DPA.

“Customer Data” has the meaning given to it in the DPA.

“Customer-Provided Equipment” means components, including equipment and software, not provided by Motorola which may be required for use of the Products and Services.

“Data Processing Addendum” or **“DPA”** means the Motorola Data Processing Addendum applicable to processing of Customer Data for US customers, as updated, supplemented, or superseded from time to time. The DPA is located at https://www.motorolasolutions.com/content/dam/msi/docs/msi-standards/terms-conditions/motorola_solutions_united_states_data_processing_addendum_online_version.pdf and is incorporated into and made a part of this Agreement for all purposes pertaining to the contents of the DPA. Where terms or provisions in the Agreement conflict with terms or provisions of the DPA, the terms or provisions of the DPA will control with respect to the contents of the DPA.

“Documentation” means the documentation for the Equipment, software Products, or data, that is delivered with the Products and Services that specifies technical and performance features, capabilities, users, or operation, including training manuals, and other deliverables, such as reports, specifications, designs, plans, drawings, analytics, or other information.

“Equipment” means hardware provided by Motorola.

“Equipment Lease-Purchase Agreement” means the agreement by which Customer finances all or a portion of the Contract Price.

“Feedback” means comments or information, in oral or written form, given to Motorola by Customer or Authorized Users, including their end users, in connection with or relating to the Products or Services;

“Fees” means charges applicable to the Products and Services.

“Integration Services” means the design, deployment, and integration Services provided by Motorola in order to design, install, set up, configure, and/or integrate the applicable Products as agreed upon by the Parties.

“Licensed Software” means licensed software which is either preinstalled on Equipment or installed on Customer-Provided Equipment and licensed to Customer by Motorola for a perpetual or other defined license term.

“Maintenance and Support Services” means the break/fix maintenance, technical support, or other Services (such as software integration Services) described in the applicable statement of work.

“Motorola Data” means data owned or licensed by Motorola and made available to Customer in connection with the Products and Services;

“Motorola Materials” means proprietary software, tools, data, and other materials, including designs, utilities, models, methodologies, systems, and specifications, which Motorola has developed or licensed from third parties (including any corrections, bug fixes, enhancements, updates, modifications, adaptations, translations, de-compilations, disassemblies, or derivative works of the

foregoing, whether made by Motorola or another party). Products and Services, Motorola Data, Third-Party Data, and Documentation, are considered Motorola Materials

“Non-Motorola Materials” means collectively, Customer or third-party software, services, hardware, content, and data that is not provided by Motorola.

“Proposal” means solution descriptions, pricing, equipment lists, statements of work (“SOW”), schedules, technical specifications, quotes, and other documents setting forth the Products and Services to be purchased by Customer and provided by Motorola. The Proposal may also include an ATP, Acceptance Test Plan, depending on the Products and Services purchased by Customer.

“Products” or **“Product”** is how the Equipment, Licensed Software, and Subscription Software being purchased by the Customer will collectively be referred to in this Agreement (collectively as “Products”, or individually as a “Product”).

“Professional Services” are Services provided by Motorola to Customer under this Agreement the nature and scope of which are more fully described in the Proposal and Section 2.2.5 of this Agreement.

“Prohibited Jurisdiction” means any jurisdiction in which the provision of such Products and Services is prohibited under applicable laws or regulations.

“Process” or **“Processing”** have the meaning given to them in the DPA

“Services” means services related to purchased Products as described in the Proposal.

“Service Completion Date” means the date of Motorola’s completion of the Services described in a Proposal.

“Service Use Data” has the meaning given to it in the DPA.

“Site” or **“Sites”** means the location where the Integration Services or Maintenance and Support Services will take place.

“Software System” means a solution that includes at least one software Product and requires Integration Services to deploy such software Product at a Customer Site or onto any Customer-Provided Equipment or Equipment provided to Customer.

“SUA” or **“SUA II”** means Motorola’s Software Upgrade Agreement program.

“Subscription Software” means licensed cloud-based software-as-a-service products and other software which is either preinstalled on Equipment or installed on Customer-Provided Equipment, but licensed to Customer by Motorola on a subscription basis.

“Third-Party Data” has the meaning given to it in the DPA.

“Term” means the term of this MCA which will commence on the Effective Date and continue until six (6) months after the later of (a) the termination, expiration, or discontinuance of services under the last Proposal in effect, or (b) the expiration of all applicable warranty periods, unless the MCA is earlier terminated as set forth herein.

Section 3. Products and Services.

3.1. Products. Motorola will (a) sell Equipment, (b) Licensed Software, and (c) Subscription Software to Customer, to the extent each is set forth in this Agreement. At any time during the Term (as defined below), Motorola may substitute any Products at no cost to Customer, if the substitute is substantially similar to the Products set forth in this Agreement.

3.2. Services.

3.2.1. Motorola will provide Services, to the extent set forth in this Agreement.

3.2.2. Integration Services; Maintenance and Support Services. Motorola will provide (a) Integration Services at the applicable Sites, agreed upon by the Parties or (b) Maintenance and Support Services, each as further described in the applicable statement of work. Maintenance, Support Services and Integration Services will each be considered “Services”, as defined above.

3.2.3. Service Proposals. The Fees for Services will be set forth in Motorola’s Quote or Proposal. A Customer point of contact will be set forth in the applicable statement of work for the Services. For purposes of clarity, each statement of work will be incorporated into, and form an integral part of, this Agreement.

3.2.4. Service Completion. Services described in a Proposal will be deemed complete upon the Service Completion Date, or as Services are renewed or terminated.

3.2.5. Professional Services

3.2.5.1. Assessment of Systems & Operations. If Customer is purchasing Professional Services to evaluate or assess networks, systems or operations, Customer acknowledges and agrees that the equipment provided by or used by Motorola to facilitate performance of the Services may impact or disrupt information systems. Except as specifically set forth in the Agreement, Motorola disclaims responsibility for costs in connection with any such disruptions of and/or damage to Customer’s or a third party’s information systems, equipment, voice transmissions, and data, including, but not limited to, denial or access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision or delivery of the Service. Motorola agrees to cooperate with Customer to schedule any such potential damage or disruption around Customer’s voice or information technology traffic and use patterns so as to reduce the risk of disruption during working hours.

3.2.5.2. Network Security. If Customer is purchasing network security assessment of network monitoring Professional Services, Customer acknowledges and agrees that Motorola does not guarantee or warrant that it will discover all of Customer’s system vulnerabilities or inefficiencies. Customer agrees not to represent to third parties that Motorola has provided such guarantee. Motorola disclaims any and all responsibility for any and all loss or costs of any kind associated with vulnerabilities or security events, whether or not they are discovered by Motorola.

3.2.5.3. Application Development. If Customer purchases software application development as part of the Professional Services, the deliverables will be licensed as described in Section 2.5 - Documentation.

3.2.6. Transport Connectivity Services. Certain Communications Systems may include one or more transport connectivity services as specified in the Proposal. In addition to the terms of this MCA, transport connectivity services shall also be governed by the terms of Motorola’s standard Transport Connectivity Addendum, a copy of which is available here: https://www.motorolasolutions.com/en_us/about/legal/transport-connectivity-addendum.html.

- 3.3. Non-Preclusion.** If, in connection with the Products and Services provided under this Agreement, Motorola performs assessments of its own, or related, products or makes recommendations, including a recommendation to purchase other products or services, nothing in this Agreement precludes such efforts nor precludes Motorola from participating in a future competitive bidding process or otherwise offering or selling the recommended products or other services to Customer. Customer represents that this paragraph does not violate its procurement standards or other laws, regulations, or policies.
- 3.4. Customer Obligations.** Customer represents that information Customer provides to Motorola in connection with receipt of Products and Services are accurate and complete in all material respects. If any assumptions in the Proposals or information provided by Customer prove to be incorrect, or if Customer fails to perform any of its obligations under this Agreement, Motorola's ability to perform its obligations may be impacted and changes to the Agreement, including the scope, Fees, and performance schedule may be required.
- 3.5. Documentation.** Products and Services may be delivered with Documentation. Documentation is and will be owned by Motorola, unless otherwise expressly agreed in an Addendum or Proposal that certain Documentation will be owned by Customer. Motorola hereby grants Customer a limited, royalty-free, worldwide, non-exclusive license to use the Documentation solely for its internal business purposes in connection with the Products and Services.
- 3.6. Motorola Tools and Equipment.** As part of delivering the Products and Services, Motorola may provide certain tools, equipment, models, and other materials of its own. Such tools and equipment will remain the sole property of Motorola unless they are to be purchased by Customer as Products and are explicitly listed on the Proposal. The tools and equipment may be held by Customer for Motorola's use without charge and may be removed from Customer's premises by Motorola at any time without restriction. Customer will safeguard all tools and equipment while in Customer's custody or control, and be liable for any loss or damage. Upon the expiration or earlier termination of this Agreement, Customer, at its expense, will return to Motorola all tools and equipment in its possession or control.
- 3.7. Authorized Users.** Customer will ensure its employees and Authorized Users comply with the terms of this Agreement and will be liable for all acts and omissions of its employees and Authorized Users. Customer is responsible for the secure management of Authorized Users' names, passwords and login credentials for access to Products and Services.
- 3.8. Export Control.** Customer, its employees, and any other Authorized Users will not access or use the Products and Services in any Prohibited Jurisdiction), and Customer will not provide access to the Products and Services to any government, entity, or individual located in a Prohibited Jurisdiction. Customer represents and warrants that (a) it and its Authorized Users are not named on any U.S. government list of persons prohibited from receiving U.S. exports, or transacting with any U.S. person; (b) it and its Authorized Users are not a national of, or a company registered in, any Prohibited Jurisdiction; (c) Customer will not permit its Authorized Users to access or use the Products or Services in violation of any U.S. or other applicable export embargoes, prohibitions or restrictions; and (d) Customer and its Authorized Users will comply with all applicable laws regarding the transmission of technical data exported from the U.S. and the country in which Customer, its employees, and the Authorized Users are located.
- 3.9.** To obtain any additional Services, Customer will issue a purchase order referring to this Agreement and the separate proposal document. Omission of reference to this Agreement in Customer's purchase order will not affect the applicability of this Agreement. Motorola's proposal may include a cover page entitled "Service Agreement" or "Installation Agreement", as applicable, and other

attachments. These cover pages and other attachments are incorporated into this Agreement by this reference.

- 3.10. Change Orders.** Unless a different change control process is agreed upon in writing by the Parties, a Party may request changes to an Addendum or a Proposal by submitting a Change Order to the other Party. If a requested change in a Change Order causes an increase or decrease in the Products or Services, the Parties by means of the Change Order will make appropriate adjustments to the Fees, project schedule, or other matters. Change Orders are effective and binding on the Parties only upon execution of the Change Order by an authorized representative of both Parties.

Section 4. Term and Termination.

- 4.1. Term.** The applicable Addendum or Proposal will set forth the Term for the Products and Services governed thereby.

- 4.1.1. Subscription Terms.** The duration of Customer's subscription commences upon delivery of the first Subscription Software (and recurring Services, if applicable) ordered under this Agreement and will continue for a twelve (12) month period or such longer period identified in a Proposal (the "**Initial Subscription Period**") and will automatically renew for additional twelve (12) month periods (each, a "**Renewal Subscription Year**"), unless either Party notifies the other of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. (The Initial Subscription Period and each Renewal Subscription Year will each be referred to herein as a "**Subscription Term**".) Motorola may increase Fees prior to any Renewal Subscription Year. In such case, Motorola will notify Customer of such proposed increase no later than thirty (30) days prior to commencement of such Renewal Subscription Year.

Unless otherwise specified in writing, additional Subscription Software or recurring Services purchased under this Agreement will (a) commence upon delivery of such Subscription Software or recurring Service, and continue until the conclusion of Customer's then-current Subscription Term (a "**Partial Subscription Year**"), and (b) automatically renew for Renewal Subscription Years thereafter, unless either Party notifies the other of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. Unless otherwise specified in writing, the Subscription Terms for all Subscription Software and recurring Services hereunder will be synchronized.

- 4.2. Termination.** Either Party may terminate the Agreement or the applicable Addendum or Proposal if the other Party breaches a material obligation under the Agreement and does not cure such breach within thirty (30) days after receipt of notice of the breach or fails to produce a cure plan within such period of time. Each Addendum and Proposal may be separately terminable as set forth therein.
- 4.3. Termination for Non-Appropriation.** In the event any identified funding is not appropriated or becomes unavailable, the Customer reserves the right to terminate this Agreement for non-appropriation upon thirty (30) days' advance written notice to Motorola. In the event of such termination, Motorola shall be entitled to compensation for all conforming goods delivered and for all services performed prior to the effective date of termination date.
- 4.4. Suspension of Services.** Motorola may promptly terminate or suspend any Products or Services under a Proposal if Motorola determines: (a) the related Product license has expired or has terminated for any reason; (b) the applicable Product is being used on a hardware platform, operating system, or version not approved by Motorola; (c) Customer fails to make any payments

when due; or (d) Customer fails to comply with any of its other obligations or otherwise delays Motorola's ability to perform.

- 4.5. Wind Down of Subscription Software.** In addition to the termination rights in this Agreement, Motorola may terminate any Subscription Term, in whole or in part, in the event Motorola plans to cease offering the applicable Subscription Software or Service to customers.
- 4.6. Effect of Termination or Expiration.** Upon termination for any reason or expiration of this Agreement, an Addendum, or a Proposal, Customer and the Authorized Users will return or destroy (at Motorola's option) all Motorola Materials and Motorola's Confidential Information in their possession or control and, as applicable, provide proof of such destruction, except that Equipment purchased by Customer should not be returned. If Customer has any outstanding payment obligations under this Agreement, Motorola may accelerate and declare all such obligations of Customer immediately due and payable by Customer. Notwithstanding the reason for termination or expiration, Customer agrees to pay Motorola for Products and Services already delivered. Customer has a duty to mitigate any damages under this Agreement, including in the event of default by Motorola and Customer's termination of this Agreement.
- 4.7. Equipment as a Service.** In the event that Customer purchases any Equipment at a price below the published list price for such Equipment in connection with Customer entering into a fixed- or minimum required-term agreement for Subscription Software, and Customer or Motorola terminates the Agreement prior to the expiration of such fixed- or minimum required-term, then Motorola will have the right to invoice Customer for, and Customer will pay, the amount of the discount to the published list price for the Equipment or such other amount set forth in writing. This Section will not limit any other remedies Motorola may have with respect to an early termination.

Section 5. Payment, Invoicing, Delivery and Risk of Loss

- 5.1.** Customer affirms they have signatory authority to execute this contract. The Contract Price of \$_____, excluding taxes, is fully committed and identified, including all subsequent years of contracted services, if applicable. The Customer will pay all invoices as received from Motorola subject to the terms of this Agreement and any changes in scope will be subject to the change order process as described in this Agreement.

Motorola acknowledges the Customer may require the issuance(s) of a purchase order or notice to proceed as part of the Customer's procurement process. However, Customer agrees that the issuance or non-issuance of a purchase order or notice to proceed does not preclude the Customer from its contractual obligations as defined in this Agreement.

- 5.2. Fees.** Fees and charges applicable to the Products and Services will be as set forth in the applicable Addendum or Proposal. Changes in the scope of Services described in a Proposal that require an adjustment to the Fees will be set forth in the applicable pricing schedule. Unless otherwise specified in the applicable Proposal, the Fees for any Services exclude expenses associated with unusual and costly Site access requirements (e.g., if Site access requires a helicopter or other equipment), and Customer will reimburse Motorola for these or other expenses incurred by Motorola in connection with the Services. The annual subscription Fee for Subscription Software and associated recurring Services may include certain one-time Fees, such as start-up fees, license fees, or other fees set forth in a Proposal. Motorola may suspend the Subscription Software and any recurring Services if Customer fails to make any payments within thirty (30) days of invoice due date when due.

5.3. Taxes. The Fees do not include any excise, sales, lease, use, property, or other taxes, assessments, duties, or regulatory charges or contribution requirements (collectively, "**Taxes**"), all of which will be paid by Customer, except as exempt by law, unless otherwise specified in a Proposal. If Motorola is required to pay any Taxes, Customer will reimburse Motorola for such Taxes (including any interest and penalties) within thirty (30) days after Customer's receipt of an invoice therefore. Customer will be solely responsible for reporting the Products for personal property tax purposes, and Motorola will be solely responsible for reporting taxes on its income and net worth.

5.4. Invoicing. Motorola will invoice Customer as described in this Agreement and Customer will pay all invoices within thirty (30) days of the invoice date or as otherwise specified in writing. In the event Customer finances the purchase of the Motorola Products and Services contemplated herein via Motorola Solutions Credit Corporation ("MSCC"), invoices for such purchase will be paid via the disbursement of the financing proceeds pursuant to the Equipment Lease - Purchase Agreement executed between the parties and the payment schedule enclosed therein shall control payment of the related invoices. Late payments will be subject to interest charges at the maximum rate permitted by law, commencing upon the due date. Motorola may invoice electronically via email, and Customer agrees to receive invoices via email at the email address set forth in a Proposal. Customer acknowledges and agrees that a purchase order or other notice to proceed is not required for payment for Products or Services.

5.5. Payment. Customer will pay invoices for the Products and Services provided under this Agreement in accordance with the invoice payment terms set forth in Section 5.4. Generally, invoices are issued after shipment of Equipment or upon Motorola's delivery of Licensed Software, or upon System Completion Date of a Software System, as applicable, but if a specific invoicing or payment schedule is set forth in the Agreement, such schedule will determine the invoicing cadence.

Motorola will have the right to suspend future deliveries of Products and Services if Customer fails to make any payments when due.

5.6. INVOICING AND SHIPPING ADDRESSES. Invoices will be sent to the Customer at the following address:

Name: _____
Address: _____
Phone: _____

E-INVOICE. To receive invoices via email:

Customer Account Number: _____
Customer Accounts Payable Email: _____
Customer CC (optional) Email: _____

The address which is the ultimate destination where the Equipment will be delivered to Customer is:

Name: _____
Address: _____

The Equipment will be shipped to the Customer at the following address (insert if this information is known):

Name: _____
Address: _____
Phone: _____

Customer may change this information by giving written notice to Motorola.

5.7. Delivery, Title and Risk of Loss. Motorola will provide to Customer the Products (and, if applicable, related Services) set forth in a Proposal, in accordance with the terms of the Agreement. Motorola will, using commercially reasonable practices, pack the ordered Equipment and ship such Equipment to the Customer address set forth in **Section 5.6** or otherwise provided by Customer in writing, using a carrier selected by Motorola.

Notwithstanding the foregoing and unless otherwise stated in a Equipment Lease - Purchase Agreement, delivery of Equipment (and any incorporated Licensed Software) will occur, and title and risk of loss for the Equipment will pass to Customer, upon shipment by Motorola in accordance with ExWorks, Motorola's premises (Incoterms 2020). Customer will pay all shipping costs, taxes, and other charges applicable to the shipment and import or export of the Products and Services, as applicable, and Customer will be responsible for reporting the Products for personal property tax purposes.

Delivery of Licensed Software for installation on Equipment or Customer-Provided Equipment will occur upon the earlier of (a) electronic delivery of the Licensed Software by Motorola, and (b) the date Motorola otherwise makes the Licensed Software available for download by Customer. If agreed upon in a Proposal, Motorola will also provide Services related to such Products. Title to Licensed Software and/or Subscription Software will not pass to Customer at any time.

5.8. Delays. Any shipping dates set forth in a Proposal are approximate, and while Motorola will make reasonable efforts to ship Products by any such estimated shipping date, Motorola will not be liable for any delay or related damages to Customer. Time for delivery will not be of the essence, and delays will not constitute grounds for cancellation, penalties, termination, or a refund.

5.9. Future Regulatory Requirements. The Parties acknowledge and agree that certain Services (i.e. cyber) are an evolving technological area and therefore, laws and regulations regarding Services may change. Changes to existing Services required to achieve regulatory compliance may be available for an additional fee. Any required changes may also impact the price for Services.

Section 6. Sites; Customer-Provided Equipment; Non-Motorola Materials.

6.1. Access to Sites. Customer will be responsible for providing all necessary permits, licenses, and other approvals necessary for the installation and use of the Products and the performance of the Services at each applicable Site, including for Motorola to perform its obligations hereunder, and for facilitating Motorola's access to the Sites. No waivers of liability will be imposed on Motorola or its subcontractors by Customer or others at Customer facilities or other Sites, but if and to the extent any such waivers are imposed, the Parties agree such waivers are void.

6.2. Site Conditions. Customer will ensure that (a) all Sites are safe and secure, (b) Site conditions meet all applicable industry and legal standards (including standards promulgated by OSHA or other governmental or regulatory bodies), (c) to the extent applicable, Sites have adequate physical space, air conditioning, and other environmental conditions, electrical power outlets, distribution, equipment, connections, and telephone or other communication lines (including modem access and interfacing networking capabilities), and (d) Sites are suitable for the installation, use, and maintenance of the Products and Services. This Agreement is predicated

upon normal soil conditions as defined by the version of E.I.A. standard RS-222 in effect on the Effective Date.

- 6.3. Site Issues.** Upon its request, which will not be unreasonably denied, Motorola will have the right to inspect the Sites and advise Customer of any deficiencies or non-conformities with the requirements of this **Section 6 – Sites; Customer-Provided Equipment; Non-Motorola Materials**. If Motorola or Customer identifies any deficiencies or non-conformities, Customer will promptly remediate such issues or the Parties will select a replacement Site. If a Party determines that a Site identified in a Proposal is not acceptable or desired, the Parties will cooperate to investigate the conditions and select a replacement Site or otherwise adjust the installation plans and specifications as necessary. A change in Site or adjustment to the installation plans and specifications may cause a change in the Fees or performance schedule under the applicable Proposal.
- 6.4. Customer-Provided Equipment.** Customer will be responsible, at its sole cost and expense, for providing and maintaining the Customer-Provided Equipment in good working order. Customer represents and warrants that it has all rights in Customer-Provided Equipment to permit Motorola to access and use the applicable Customer-Provided Equipment to provide the Products and Services under this Agreement, and such access and use will not violate any laws or infringe any third-party rights (including intellectual property rights). Customer (and not Motorola) will be fully liable for Customer-Provided Equipment, and Customer will immediately notify Motorola of any Customer-Provided Equipment damage, loss, change, or theft that may impact Motorola's ability to provide the Products and Services under this Agreement, and Customer acknowledges that any such events may cause a change in the Fees or performance schedule under the applicable Proposal.
- 6.5. Non-Motorola Materials.** In certain instances, Customer may be permitted to access, use, or integrate Non-Motorola Materials with or through the Products and Services. If Customer accesses, uses, or integrates any Non-Motorola Materials with the Products or Services, Customer will first obtain all necessary rights and licenses to permit Customer's and its Authorized Users' use of the Non-Motorola Materials in connection with the Products and Services. Customer will also obtain the necessary rights for Motorola to use such Non-Motorola Materials in connection with providing the Products and Services, including the right for Motorola to access, store, and process such Non-Motorola Materials (e.g., in connection with Subscription Software), and to otherwise enable interoperation with the Products and Services. Customer represents and warrants that it will obtain the foregoing rights and licenses prior to accessing, using, or integrating the applicable Non-Motorola Materials with the Products and Services, and that Customer and its Authorized Users will comply with any terms and conditions applicable to such Non-Motorola Materials. If any Non-Motorola Materials requires access to Customer Data (as defined below), Customer hereby authorizes Motorola to allow the provider of such Non-Motorola Materials to access Customer Data, in connection with the interoperation of such Non-Motorola Materials with the Products and Services.
- 6.6.** Customer acknowledges and agrees that Motorola is not responsible for, and makes no representations or warranties with respect to, the Non-Motorola Materials (including any disclosure, modification, or deletion of Customer Data resulting from use of Non-Motorola Materials or failure to properly interoperate with the Products and Services). If Customer receives notice that any Non-Motorola Materials must be removed, modified, or disabled within the Products or Services, Customer will promptly do so. Motorola will have the right to disable or remove Non-Motorola Materials if Motorola believes a violation of law, third-party rights, or Motorola's policies is likely to occur, or if such Non-Motorola Materials poses or may pose a security or other risk or

adverse impact to the Products or Services, Motorola, Motorola's systems, or any third party (including other Motorola customers).

- 6.7.** Motorola may provide certain Non-Motorola Materials as an authorized sales representative of a third party as set out in a Proposal. As an authorized sales representative, the third party's terms and conditions, as set forth in the Proposal, will apply to any such sales. Any orders for such Non-Motorola Materials will be filled by the third party. Nothing in this Section will limit the exclusions set forth in **Section 8.2 – Intellectual Property Infringement**.
- 6.8. End User Licenses.** Notwithstanding any provision to the contrary in the Agreement, certain Non-Motorola Materials software are governed by a separate license, EULA, or other agreement, including terms governing third-party equipment or software, such as open source software, included in the Products and Services. Customer will comply, and ensure its Authorized Users comply, with any such additional terms applicable to third-party equipment or software. Third party software flow-down terms applicable to Motorola products are located at the following site: https://www.motorolasolutions.com/en_us/about/legal/motorola-solutions-customer-terms/flow-down-terms.html
- 6.9. Prohibited Use.** Customer will not integrate or use, or permit a third party or an Authorized User to integrate or use, any Non-Motorola Materials with or in connection with a Software System or other software Product provided by Motorola under this Agreement, without the express written permission of Motorola.
- 6.10. API Support.** Motorola will use commercially reasonable efforts to maintain its Application Programming Interface ("API") offered solely in connection with any Software System. APIs will evolve and mature over time, requiring changes and updates. Motorola will use reasonable efforts to continue supporting any version of an API for 6 months after such version is introduced, but if Motorola determines, in its sole discretion, to discontinue support of an API for any reason, Motorola will provide reasonable advance notification to Customer. If an API presents a security risk, Motorola may discontinue an API without prior notice.
- 6.11. Support of Downloaded Clients.** If Customer purchases any software Product that requires a client installed locally on any Customer-Provided Equipment or Equipment in possession of Customer, Customer will be responsible for downloading and installing the current version of such client, as it may be updated from time to time. Motorola will use reasonable efforts to continue supporting any version of a client for forty-five (45) days following its release, but Motorola may update the current version of its client at any time, including for bug fixes, product improvements, and feature updates, and Motorola makes no representations or warranties that any software Product will support prior versions of a client.

Section 7. Representations and Warranties.

- 7.1. Mutual Representations and Warranties.** Each Party represents and warrants to the other Party that (a) it has the right to enter into the Agreement and perform its obligations hereunder, and (b) the Agreement will be binding on such Party.
- 7.2. Communications System Warranty.** Motorola represents and warrants that, on the date of System Acceptance, (a) the Communications System will perform in accordance with the descriptions in the applicable Proposal in all material respects, and (b) if Customer has purchased any Equipment or Motorola Licensed Software (but, for clarity, excluding Subscription Software) as part of such Communications System, the warranty period applicable to such Equipment and Motorola Licensed Software will continue for a period of one (1) year commencing upon System Acceptance (the "Warranty Period").

7.3. During the Warranty Period, in addition to warranty services, Motorola will provide Maintenance and Support Services for the Equipment and support for the Motorola Licensed Software pursuant to the applicable maintenance and support Proposal. Support for the Motorola Licensed Software will be in accordance with Motorola's established Software Support Policy ("SwSP"). Copies of the SwSP can be found at https://www.motorolasolutions.com/en_us/about/legal/motorola-solutions-customer-terms/software_policy.html, a copy of which is available to Customer upon written request. If Customer wishes to purchase (a) additional Maintenance and Support Services during the Warranty Period; or (b) continue or expand maintenance, software support, installation, and/or Motorola's Lifecycle Management Services ("LMS") after the Warranty Period, Motorola will provide the description of and pricing for such services in a separate proposal document and such terms will be agreed upon in a Proposal. Unless otherwise agreed by the Parties in writing, the terms and conditions in this Agreement applicable to maintenance, support, installation, and/or LMS, will be included in the Maintenance and Support Addendum, LMS Addendum, the applicable Proposals, and the proposal (if applicable). These collective terms will govern the provision of such Services.

7.4. On-Premises Software System Warranty. Motorola represents and warrants that, on the System Completion Date, or on the applicable Product Completion Date for a specific Product within such on-premises Software System, if earlier, (a) such Software System or Product will perform in accordance with the descriptions in the applicable Proposals in all material respects, and (b) if Customer has purchased any Equipment or Motorola Licensed Software (but, for clarity, excluding Subscription Software) as part of such on-premises Software System, the warranty period applicable to such Equipment and Motorola Licensed Software will continue for a period of one (1) year commencing upon the System Completion Date for the Software System that includes such Products, or on the applicable Product Completion Date, if earlier.

7.4.1. On-premises Software Systems as a service and cloud hosted Software Systems are provided as a service and accordingly do not qualify for the On-premises Software System Warranty. System completion, however, for each of these solutions is determined in accordance with **Section 12.2 Software System Completion** below.

7.5. Motorola Warranties - Services. Subject to the disclaimers and exclusions below, Motorola represents and warrants that (a) Services will be provided in a good and workmanlike manner and will conform in all material respects to the descriptions in the applicable Proposal; and (b) for a period of ninety (90) days commencing upon the Service Completion Date for one-time Services, the Services will be free of material defects in materials and workmanship. Other than as set forth in subsection (a) above, recurring Services are not warranted but rather will be subject to the requirements of the applicable Addendum or Proposal.

7.6. Motorola Warranties - Equipment. Subject to the disclaimers and exclusions set forth below, (a) for a period of one (1) year commencing upon the delivery of Motorola-manufactured Equipment under **Section 5.7 – Delivery, Title and Risk of Loss**, Motorola represents and warrants that such Motorola-manufactured Equipment, under normal use, will be free from material defects in materials and workmanship; and (b) The warranties applicable to Motorola-manufactured Equipment set forth in herein shall be applicable to all radio Equipment purchased hereunder whether or not such Equipment was manufactured by Motorola.

7.7. Motorola Licensed Software Warranty. Unless otherwise stated in the License Agreement, for a period of ninety (90) days commencing upon the delivery of Motorola-owned Licensed Software, Motorola represents and warrants that such Licensed Software, when used in accordance with the Documentation and the Agreement, will be free from reproducible defects that prevent operation of features critical to the primary functionality or successful operation of the Motorola-developed Licensed Software (as determined by Motorola)

7.7.1. As Customer's sole and exclusive remedy for any breach of the Motorola Licensed Software Warranty, Motorola will use commercially reasonable efforts to remedy the material defect in the applicable Licensed Software; provided, however, that if Motorola does not remedy such material defect within a reasonable time, then at Motorola's sole option, Motorola will either replace the defective Licensed Software with functionally-equivalent software, provide substitute software to Customer, or terminate the applicable software license and refund any paid license fees to Customer on a pro-rata basis.

7.7.2. For clarity, the Motorola Licensed Software Warranty applies only to the most current version of the Licensed Software issued by Motorola, and issuance of updated versions of any Licensed Software does not result in a renewal or extension of the Motorola Licensed Software Warranty beyond the ninety (90) day warranty period.

7.8. ADDITIONAL WARRANTY EXCLUSIONS. NOTWITHSTANDING ANY PROVISION OF THE AGREEMENT TO THE CONTRARY, MOTOROLA WILL HAVE NO LIABILITY FOR (A) DEFECTS IN OR DAMAGE TO PRODUCTS RESULTING FROM USE OTHER THAN IN THE NORMAL AUTHORIZED MANNER, OR FROM ACCIDENT, LIQUIDS, OR NEGLECT; (B) TESTING, MAINTENANCE, REPAIR, INSTALLATION, OR MODIFICATION BY PARTIES OTHER THAN MOTOROLA; (C) CUSTOMER'S OR ANY AUTHORIZED USER'S FAILURE TO COMPLY WITH INDUSTRY AND OSHA OR OTHER LEGAL STANDARDS; (D) DAMAGE TO RADIO ANTENNAS, UNLESS CAUSED BY DEFECTS IN MATERIAL OR WORKMANSHIP; (E) EQUIPMENT WITH NO SERIAL NUMBER; (F) BATTERIES OR CONSUMABLES; (G) FREIGHT COSTS FOR SHIPMENT TO REPAIR DEPOTS; (H) COSMETIC DAMAGE THAT DOES NOT AFFECT OPERATION; (I) NORMAL WEAR AND TEAR; (J) ISSUES OR OBSOLESCENCE OF LICENSED SOFTWARE DUE TO CHANGES IN CUSTOMER OR AUTHORIZED USER REQUIREMENTS, EQUIPMENT, OR SYSTEMS; (K) TRACKING AND LOCATION-BASED SERVICES; OR (L) BETA SERVICES.

7.9. Warranty Claims; Remedies. To assert a warranty claim, Customer must notify Motorola in writing of the claim prior to the expiration of any warranty period set forth in this Agreement. Unless a different remedy is otherwise expressly set forth herein, upon receipt of such claim, Motorola will investigate the claim and use commercially reasonable efforts to repair or replace any confirmed materially non-conforming Product or re-perform any non-conforming Service, at its option. Such remedies are Customer's sole and exclusive remedies for Motorola's breach of a warranty. Motorola's warranties are extended by Motorola to Customer only, and are not assignable or transferable.

7.10. Pass-Through Warranties. Notwithstanding any provision of this Agreement to the contrary, Motorola will have no liability for third-party software or hardware provided by Motorola; provided, however, that to the extent offered by third-party providers of software or hardware and to the extent permitted by law, Motorola will pass through express warranties provided by such third parties.

7.11. WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS AND PASS THROUGH WARRANTIES IN THIS AGREEMENT, PRODUCTS AND SERVICES PURCHASED HEREUNDER ARE PROVIDED "AS IS" AND WITH ALL FAULTS. WARRANTIES SET FORTH IN THE AGREEMENT ARE THE COMPLETE WARRANTIES FOR THE PRODUCTS AND SERVICES AND MOTOROLA DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND QUALITY. MOTOROLA DOES NOT REPRESENT OR WARRANT THAT USE OF THE PRODUCTS AND SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR FREE OF SECURITY VULNERABILITIES, OR THAT THEY WILL MEET CUSTOMER'S PARTICULAR REQUIREMENTS.

Section 8. Indemnification.

- 8.1. General Indemnity.** Motorola will defend, indemnify, and hold Customer harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual third-party claim, demand, action, or proceeding (“Claim”) for personal injury, death, or direct damage to tangible property to the extent caused by Motorola’s negligence, gross negligence or willful misconduct while performing its duties under this Agreement, except to the extent the claim arises from Customer’s negligence or willful misconduct. Motorola’s duties under this **Section 8.1 – General Indemnity** are conditioned upon: (a) Customer promptly notifying Motorola in writing of the Claim; (b) Motorola having sole control of the defense of the suit and all negotiations for its settlement or compromise to the extent allowed by applicable law; and (c) Customer cooperating with Motorola and, if requested by Motorola, providing reasonable assistance in the defense of the Claim.
- 8.2. Intellectual Property Infringement.** Motorola will defend Customer against any third-party claim alleging that a Motorola-developed or manufactured Product or Service (the “Infringing Product”) directly infringes a United States patent or copyright (“Infringement Claim”), and Motorola will pay all damages finally awarded against Customer by a court of competent jurisdiction for an Infringement Claim, or agreed to in writing by Motorola in settlement of an Infringement Claim. Motorola’s duties under this **Section 8.2 – Intellectual Property Infringement** are conditioned upon: (a) Customer promptly notifying Motorola in writing of the Infringement Claim; (b) Motorola having sole control of the defense of the suit and all negotiations for its settlement or compromise; and (c) Customer cooperating with Motorola and, if requested by Motorola, providing reasonable assistance in the defense of the Infringement Claim.
- 8.2.1.** If an Infringement Claim occurs, or in Motorola’s opinion is likely to occur, Motorola may at its option and expense: (a) procure for Customer the right to continue using the Infringing Product; (b) replace or modify the Infringing Product so that it becomes non-infringing; or (c) grant Customer (i) a prorated refund of any amounts pre-paid for the Infringing Product (if the Infringing Product is a software Product, i.e., Licensed Software or Subscription Software) or (ii) a credit for the Infringing Product, less a reasonable charge for depreciation (if the Infringing Product is Equipment, including Equipment with embedded software).
- 8.2.2.** In addition to the other damages disclaimed under this Agreement, Motorola will have no duty to defend or indemnify Customer for any Infringement Claim that arises from or is based upon: (a) Customer Data, Customer-Provided Equipment, Non-Motorola Materials, or third-party equipment, hardware, software, data, or other third-party materials; (b) the combination of the Product or Service with any products or materials not provided by Motorola; (c) a Product or Service designed, modified, or manufactured in accordance with Customer’s designs, specifications, guidelines or instructions; (d) a modification of the Product or Service by a party other than Motorola; (e) use of the Product or Service in a manner for which the Product or Service was not designed or that is inconsistent with the terms of this Agreement; or (f) the failure by Customer to use or install an update to the Product or Service that is intended to correct the claimed infringement. In no event will Motorola’s liability resulting from an Infringement Claim extend in any way to any payments due on a royalty basis, other than a reasonable royalty based upon revenue derived by Motorola from Customer from sales or license of the Infringing Product.
- 8.2.3.** This **Section 8.2 – Intellectual Property Infringement** provides Customer’s sole and exclusive remedies and Motorola’s entire liability in the event of an Infringement Claim.
- 8.3. Customer Indemnity.** Reserved

Section 9. Limitation of Liability.

9.1. EXCEPT FOR PERSONAL INJURY OR DEATH, THE TOTAL AGGREGATE LIABILITY OF MOTOROLA, ITS AFFILIATES, AND ITS AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, SUBCONTRACTORS, AGENTS, SUCCESSORS, AND ASSIGNS (COLLECTIVELY, THE "MOTOROLA PARTIES"), WHETHER BASED ON A CLAIM IN CONTRACT OR IN TORT, LAW OR EQUITY, RELATING TO OR ARISING OUT OF THE AGREEMENT WILL NOT EXCEED THE FEES, OR PORTION OF FEES, RELATED TO THE PRODUCT OR INTEGRATION SERVICE UNDER WHICH THE CLAIM AROSE. WITH RESPECT TO ANY SUBSCRIPTION SOFTWARE OR ANY RECURRING SERVICES, THE MOTOROLA PARTIES' TOTAL AGGREGATE LIABILITY FOR ALL CLAIMS RELATED TO SUBSCRIPTION SOFTWARE OR RECURRING SERVICES WILL NOT EXCEED THE TOTAL FEES PAID FOR THE APPLICABLE SUBSCRIPTION SOFTWARE OR RECURRING SERVICE DURING THE CONSECUTIVE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT FROM WHICH THE FIRST CLAIM AROSE. EXCEPT FOR PERSONAL INJURY OR DEATH, THE MOTOROLA PARTIES WILL NOT BE LIABLE IN CONNECTION WITH THIS AGREEMENT (WHETHER UNDER MOTOROLA'S INDEMNITY OBLIGATIONS, A CAUSE OF ACTION FOR BREACH OF CONTRACT, UNDER TORT THEORY, OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOST PROFITS OR REVENUES, EVEN IF MOTOROLA HAS BEEN ADVISED BY CUSTOMER OR ANY THIRD PARTY OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES AND WHETHER OR NOT SUCH DAMAGES OR LOSSES ARE FORESEEABLE.

9.2. EXCLUSIONS FROM LIABILITY. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, MOTOROLA WILL HAVE NO LIABILITY FOR DAMAGES ARISING OUT OF (A) CUSTOMER DATA, INCLUDING ITS TRANSMISSION TO MOTOROLA, OR ANY OTHER DATA AVAILABLE THROUGH THE PRODUCTS OR SERVICES; (B) CUSTOMER-PROVIDED EQUIPMENT OR SITES; NON-MOTOROLA MATERIALS; THIRD-PARTY EQUIPMENT, HARDWARE, SOFTWARE, DATA, OR CONTENT; OR UNKNOWN OR UNAUTHORIZED COMBINATION OF PRODUCTS AND SERVICES ; (C) LOSS OF DATA, HACKING, RANSOMWARE, THIRD-PARTY ATTACKS OR DEMANDS; (D) MODIFICATION OF PRODUCTS OR SERVICES NOT AUTHORIZED BY MOTOROLA; (E) RECOMMENDATIONS PROVIDED IN CONNECTION WITH THE PRODUCTS AND SERVICES PROVIDED UNDER THIS AGREEMENT; (F) DATA RECOVERY SERVICES OR DATABASE MODIFICATIONS; OR (G) CUSTOMER'S OR ANY AUTHORIZED USER'S BREACH OF THIS AGREEMENT OR MISUSE OF THE PRODUCTS AND SERVICES.

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

9.3 Statute of Limitations. Customer may not bring any claims against a Motorola Party in connection with this Agreement or the Products and Services more than one (1) year after the date of accrual of the cause of action.

Section 10. Confidentiality.

- 10.1. Confidential Information.** In order to be considered Confidential Information, information that is disclosed orally must be identified as confidential at the time of disclosure and confirmed by disclosing party ("Discloser") by submitting a written document to receiving party ("Recipient") within thirty (30) days after such disclosure. The written document must contain a summary of the Confidential Information disclosed with enough specificity for identification purpose and must be labeled or marked as confidential or its equivalent.
- 10.2. Obligations of Confidentiality.** During the Term and for a period of three (3) years from the expiration or termination of this Agreement, Recipient will (a) not disclose Confidential Information to any third party, except as expressly permitted in this **Section 10 - Confidentiality**; (b) restrict disclosure of Confidential Information to only those employees, agents or consultants who must access the Confidential Information for the purpose of providing Services and who are bound by confidentiality terms substantially similar to those in this Agreement and licenses; (c) not copy, reproduce, reverse engineer, decompile or disassemble any Confidential Information; (d) use the same degree of care as for its own information of like importance, but no less than reasonable care to safeguard against disclosure; (e) promptly notify Discloser upon discovery of any unauthorized use or disclosure of the Confidential Information and take reasonable steps to regain possession of the Confidential Information and prevent further unauthorized actions or other breach of this Section; and (f) only use the Confidential Information as needed to fulfill its obligations and secure its rights under this Agreement.
- 10.3. Exceptions.** Recipient may disclose Confidential Information to the extent required by law, or a judicial or legislative order or proceeding. Recipient is not obligated to maintain as confidential any information that Recipient can demonstrate by documentation (a) is publicly known or available prior to without breach of this Agreement; (b) is lawfully obtained; or (c) is independently known or developed by Recipient without the use of, or reference to, any of Discloser's Confidential Information or any breach of this Agreement.
- 10.4. Ownership of Confidential Information.** All Confidential Information is and will remain the property of Discloser, and will not be copied or reproduced without written permission. Within ten (10) days of receipt of Discloser's written request, Recipient will return or destroy all Confidential Information to Discloser, or certify in writing that all such Confidential Information has been destroyed. However, Recipient may retain (a) one (1) archival copy for use only in case of a dispute concerning this Agreement, and (b) Confidential Information that has been automatically stored in accordance with Recipient's standard backup or recordkeeping procedures. Recipient will remain subject to the obligations of this Agreement with respect to any Confidential Information retained

subject to clauses (a) or (b). No license, express or implied, in the Confidential Information is granted to the Recipient other than to use it in the manner, and to the extent authorized by this Agreement. Discloser represents and warrants that it is authorized to disclose any Confidential Information it discloses pursuant to this Agreement.

Section 11. Proprietary Rights; Data; Feedback.

11.1. Motorola Materials. Customer acknowledges that Motorola may use or provide Customer with access to “Motorola Materials”. Except when Motorola has expressly transferred title or other interest to Customer by way of an Addendum, the Motorola Materials are the property of Motorola or its licensors, and Motorola or its licensors retain all right, title and interest in and to the Motorola Materials (including, all rights in patents, copyrights, trademarks, trade names, trade secrets, know-how, other intellectual property and proprietary rights, and all associated goodwill and moral rights).

This Agreement does not grant to Customer any shared development rights in or to any Motorola Materials or other intellectual property, and Customer agrees to execute any documents and take any other actions reasonably requested by Motorola to effectuate the foregoing. Motorola and its licensors reserve all rights not expressly granted to Customer, and no rights, other than those expressly granted herein, are granted to Customer by implication, estoppel or otherwise. Customer will not modify, disassemble, reverse engineer, derive source code or create derivative works from, merge with other software, distribute, sublicense, sell, or export the Products and Services or other Motorola Materials, or permit any third party to do so.

11.2. Ownership of Customer Data. Customer retains all right, title and interest, including intellectual property rights, if any, in and to Customer Data. Motorola acquires no rights to Customer Data except those rights granted under this Agreement including the right to Process and use the Customer Data as set forth in the DPA.

11.3. Data Retention and Deletion. Except as expressly provided otherwise under the DPA, Motorola will delete all Customer Data following termination or expiration of this MCA or the applicable Addendum or Proposal, with such deletion to occur no later than ninety (90) days following the applicable date of termination or expiration, unless otherwise required to comply with applicable law. Any requests for the exportation or download of Customer Data must be made by Customer to Motorola in writing before expiration or termination, subject to **Section 15.9 – Notices**. Motorola will have no obligation to retain such Customer Data beyond expiration or termination unless the Customer has purchased extended storage from Motorola through a mutually executed Proposal.

11.4. Service Use Data. Customer understands and agrees that Motorola may collect and use Service Use Data for its own purposes, and may disclose Service Use Data to third parties. It is Customer’s responsibility to notify Authorized Users of Motorola’s collection and use of Service Use Data and to obtain any required consents, provide all necessary notices, and meet any other applicable legal requirements with respect to such collection and use, and Customer represents and warrants to Motorola that it has complied and will continue to comply with this Section.

11.5. Third-Party Data and Motorola Data. Customer will not, and will use reasonable efforts to ensure its Authorized Users will not: (a) use the Motorola Data or Third-Party Data for any purpose other than Customer’s internal business purposes; (b) disclose the data to third parties; (c) “white label” such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (d) use such data in violation of applicable laws; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data; or (f) modify such data or combine it with Customer Data or other

data or use the data to build databases. Additional restrictions may be set forth in the applicable Addendum.

- 11.5.1.** Any rights granted to Customer or Authorized Users with respect to Motorola Data or Third-Party Data will immediately terminate upon termination or expiration of the applicable Addendum, Proposal, or this MCA. Further, Motorola or the applicable Third-Party Data provider may suspend, change, or terminate Customer's or any Authorized User's access to Motorola Data or Third-Party Data if Motorola or such Third-Party Data provider believes Customer's or the Authorized User's use of the data violates the Agreement, applicable law or Motorola's agreement with the applicable Third-Party Data provider.
- 11.5.2.** Upon termination of Customer's rights to use any Motorola Data or Third-Party Data, Customer and all Authorized Users will immediately discontinue use of such data, delete all copies of such data, and certify such deletion to Motorola. Notwithstanding any provision of the Agreement to the contrary, Motorola will have no liability for Third-Party Data or Motorola Data available through the Products and Services. Motorola and its Third-Party Data providers reserve all rights in and to Motorola Data and Third-Party Data not expressly granted in an Addendum or Proposal.
- 11.6. Feedback.** Any Feedback provided by Customer is entirely voluntary, and will not create any confidentiality obligation for Motorola, even if designated as confidential by Customer. Motorola may use, reproduce, license, and otherwise distribute and exploit the Feedback without any obligation or payment to Customer or Authorized Users and Customer represents and warrants that it has obtained all necessary rights and consents to grant Motorola the foregoing rights.
- 11.7. Improvements; Products and Services.** The Parties agree that, notwithstanding any provision of this Agreement to the contrary, all fixes, modifications and improvements to the Services or Products conceived of or made by or on behalf of Motorola that are based either in whole or in part on the Feedback, Customer Data, or Service Use Data (or otherwise) are the exclusive property of Motorola and all right, title and interest in and to such fixes, modifications or improvements will vest solely in Motorola. Customer agrees to execute any written documents necessary to assign any intellectual property or other rights it may have in such fixes, modifications or improvements to Motorola.

Section 12. Acceptance

12.1. Communications System Acceptance.

- 12.1.1.** Any Communications System described in the Proposal hereunder (including the Products, Integration Services, and all other components thereof) will be deemed completed upon successful completion of the acceptance procedures ("Acceptance Tests") set forth in the Acceptance Test Plan ("System Acceptance"). Motorola will notify Customer at least ten (10) days before the Communications System testing commences. Upon System Acceptance, the Parties will memorialize this event by promptly executing a certificate documenting such System Acceptance as set forth in Exhibit C. If the Acceptance Test Plan includes separate tests for individual sub-Systems or phases of the Communications System, acceptance of the individual sub-System or phase will occur upon the successful completion of the Acceptance Tests for the sub-Communications System or phase, and the Parties will promptly execute an acceptance certificate for the sub-Communications System or phase. If Customer believes the Communications System has failed the completed Acceptance Tests, Customer will provide to Motorola a written notice that includes the specific details of the failure. If Customer does not provide to Motorola a failure notice within thirty (30) days after completion of the Acceptance Tests, System Acceptance will be deemed to have occurred as of the completion of the

Acceptance Tests. Minor omissions or variances in the Communications System that do not materially impair the operation of the Communications System as a whole will not postpone System Acceptance or sub-Communications System acceptance, but will be corrected according to a mutually agreed punch list schedule. This Section applies to Products purchased as part of a Communications System notwithstanding any conflicting delivery provisions within this Agreement and this Section will control over such other delivery provisions to the extent of a conflict.

12.1.2. Beneficial Use. Customer acknowledges that Motorola's ability to perform its implementation and testing responsibilities may be impeded if Customer begins using the Communications System before System Acceptance.

12.1.3. Customer shall not commence using the system before System Acceptance without Motorola's prior written authorization, which will not be unreasonably withheld. Motorola is not responsible for Communications System performance deficiencies that occur prior to System Acceptance or written authorized use. Upon the date Customer begins using the Communications System, Customer assumes responsibility for the use and operation of the Communications System.

12.2 Software System Completion. Any Software System described in the Proposal (including the Products, Integration Services, and all other components thereof) will be deemed completed upon Customer's (or the applicable Authorized User's) Beneficial Use of each Product that is included in the Software System (unless alternative acceptance procedures are set forth in the Proposal) (the "System Completion Date"). Customer will not unreasonably delay Beneficial Use of any Product within a Software System, and in any event, the Parties agree that Beneficial Use of a Product will be deemed to have occurred thirty (30) days after functional demonstration. For clarity, if a Software System is comprised of more than one Product, Motorola may notify Customer that all Integration Services for a particular Product within the Software System have been completed, and Customer may have Beneficial Use of such Product prior to having Beneficial Use of other Products in the Software System, or of the Software System as a whole. In such case, the Integration Services applicable to such Product will be deemed complete upon Customer's Beneficial Use of the Product ("Product Completion Date"), which may occur before the System Completion Date. As used in this Section, "Beneficial Use" means use by Customer or at least one (1) Authorized User of the material features and functionalities of a Product within a Software System, in material conformance with Product descriptions in the Proposal. This Section applies to Products purchased as part of a Software System notwithstanding any conflicting delivery provisions within this Agreement, and will control over such other delivery provisions to the extent of a conflict.

Section 13. Force Majeure; Delays Caused by Customer.

13.1. Force Majeure. Except for Customer's payment obligations hereunder, neither Party will be responsible for nonperformance or delayed performance due to events outside of its reasonable control. If performance will be significantly delayed, the affected Party will provide notice to the other Party, and the Parties will agree (in writing) upon a reasonable extension to any applicable performance schedule.

13.2. Delays Caused by Customer. Motorola's performance of the Products and Services will be excused for delays caused by Customer or its Authorized Users or subcontractors, or by failure of any assumptions set forth in this Agreement (including in any Addendum or Proposal). In the event of a delay under this **Section 13.2 – Delays Caused by Customer**, (a) Customer will continue to pay the Fees as required hereunder, (b) the Parties will agree (in writing) upon a reasonable extension to any applicable performance schedule, and (c) Customer will compensate Motorola for its out-of-pocket costs incurred due to the delay (including those incurred by Motorola's affiliates, vendors, and subcontractors).

Section 14. Disputes. The Parties will use the following procedure to resolve any disputes relating to or arising out of this Agreement (each, a “Dispute”):

- 14.1. Governing Law.** All matters relating to or arising out of the Agreement are governed by the laws of the State of Illinois, unless Customer is the United States Government (or an agency thereof) or a state government or state agency or local municipality within the United States, in which case all matters relating to or arising out of the Agreement will be governed by the laws of the State in which the Products and Services are provided. The terms of the U.N. Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act will not apply.
- 14.2. Negotiation; Mediation.** The Parties will attempt to timely resolve the Dispute promptly through good faith negotiations. Either Party may initiate dispute resolution procedures by sending a notice of Dispute (“Notice of Dispute”) to the other Party. The Parties will choose an independent mediator within thirty (30) days of such Notice of Mediation. Neither Party may unreasonably withhold consent to the selection of a mediator, but if the Parties are unable to agree upon a mediator, either Party may request that the American Arbitration Association nominate a mediator. Each Party will bear its own costs of mediation, but the Parties will share the cost of the mediator equally. Unless otherwise agreed in writing, all in person meetings under this **Section 14.2 – Negotiation; Mediation** will take place in Chicago, Illinois, and all communication relating to the Dispute resolution will be maintained in strict confidence by the Parties. Notwithstanding the foregoing, any Dispute arising from or relating to Motorola’s intellectual property rights must be decided by a court of competent jurisdiction, in accordance with **Section 14.3 – Litigation, Venue, Jurisdiction** below.
- 14.3. Litigation, Venue, Jurisdiction.** If the Dispute has not been resolved by mediation within sixty (60) days from the Notice of Mediation, either Party may submit the Dispute exclusively to a court in Cook County, Illinois, or in the case the Customer is the United States, a state agency, or local municipality, then the appropriate court in the State in which the Products and Services are provided. Each Party expressly consents to the exclusive jurisdiction of such courts for resolution of any Dispute and to enforce the outcome of any mediation.

Section 15. General.

- 15.1. Compliance with Laws.** Each Party will comply with applicable laws in connection with the performance of its obligations under this Agreement, including that Customer will ensure its and its Authorized Users’ use of the Products and Services complies with law (including privacy laws), and Customer will obtain any FCC and other licenses or authorizations (including licenses or authorizations required by foreign regulatory bodies) required for its and its Authorized Users’ use of the Products and Services. Motorola may, at its discretion, cease providing or otherwise modify Products and Services (or any terms related thereto in an Addendum or Proposal), in order to comply with any changes in applicable law.
- 15.2. Audit; Monitoring.** Motorola will have the right to monitor and audit use of the Products, including an audit of total user licenses credentialed by Customer for any Subscription Software, which may also include access by Motorola to Customer Data and Service Use Data. Customer will provide notice of such monitoring to its Authorized Users and obtain any required consents, including individual end users, and will cooperate with Motorola in any monitoring or audit. Customer will maintain during the Term, and for two (2) years thereafter, accurate records relating to any software licenses granted under this Agreement to verify compliance with this Agreement. Motorola or a third party (“Auditor”) may inspect Customer’s and, as applicable, Authorized Users’ premises, books, and records. Motorola will pay expenses and costs of the Auditor, unless Customer is found to be in violation of the terms of the Agreement, in which case Customer will be

responsible for such expenses and costs. In the event Motorola determines that Customer's usage of the Subscription Software during the applicable Subscription Term exceeded the total number of licenses purchased by Customer, Motorola may invoice Customer for the additional licenses used by Customer, pro-rated for each additional license from the date such license was activated, and Customer will pay such invoice in accordance with the payment terms in the Agreement.

15.3. Assignment and Subcontracting. Neither Party may assign or otherwise transfer this Agreement without the prior written approval of the other Party. Motorola may assign or otherwise transfer this Agreement or any of its rights or obligations under this Agreement without consent (a) for financing purposes, (b) in connection with a merger, acquisition or sale of all or substantially all of its assets, (c) as part of a corporate reorganization, or (d) to a subsidiary corporation. Subject to the foregoing, this Agreement will be binding upon the Parties and their respective successors and assigns. Motorola may subcontract any of the work, but subcontracting will not relieve Motorola of its duties under this Agreement.

15.4. Waiver. A delay or omission by either Party to exercise any right under this Agreement will not be construed to be a waiver of such right. A waiver by either Party of any of the obligations to be performed by the other, or any breach thereof, will not be construed to be a waiver of any succeeding breach or of any other obligation. All waivers must be in writing and signed by the Party waiving its rights.

15.5. Severability. If any provision of the Agreement is found by a court of competent jurisdiction to be invalid, illegal, or otherwise unenforceable, such provision will be deemed to be modified to reflect as nearly as possible the original intentions of the Parties in accordance with applicable law. The remaining provisions of this Agreement will not be affected, and each such provision will be valid and enforceable to the full extent permitted by applicable law.

15.6. Independent Contractors. Each Party will perform its duties under this Agreement as an independent contractor. The Parties and their personnel will not be considered to be employees or agents of the other Party. Nothing in this Agreement will be interpreted as granting either Party the right or authority to make commitments of any kind for the other. This Agreement will not constitute, create, or be interpreted as a joint venture, partnership, or formal business organization of any kind.

15.7. Third-Party Beneficiaries. The Agreement is entered into solely between, and may be enforced only by, the Parties. Each Party intends that the Agreement will not benefit, or create any right or cause of action in or on behalf of, any entity other than the Parties. Notwithstanding the foregoing, a licensor or supplier of third-party software included in the software Products will be a direct and intended third-party beneficiary of this Agreement.

15.8. Interpretation. The section headings in this Agreement are included only for convenience. The words "including" and "include" will be deemed to be followed by the phrase "without limitation". This Agreement will be fairly interpreted in accordance with its terms and conditions and not for or against either Party.

15.9. Notices. Notices required under this Agreement to be given by one Party to the other must be in writing and either personally delivered or sent to the address provided by the other Party by certified mail, return receipt requested and postage prepaid (or by a recognized courier service, such as FedEx, UPS, or DHL), and will be effective upon receipt.

15.10. Cumulative Remedies. Except as specifically stated in this Agreement, all remedies provided for in this Agreement will be cumulative and in addition to, and not in lieu of, any other remedies available to either Party at law, in equity, by contract, or otherwise. Except as specifically

stated in this Agreement, the election by a Party of any remedy provided for in this Agreement or otherwise available to such Party will not preclude such Party from pursuing any other remedies available to such Party at law, in equity, by contract, or otherwise.

15.11. Survival. The following provisions will survive the expiration or termination of this Agreement for any reason: Section 3.4 – Customer Obligations; Section 4.6 – Effect of Termination or Expiration; Section 5 – Payment and Invoicing; Section 7.11 – Warranty Disclaimer; Section 8.3 – Customer Indemnity; Section 9 – Limitation of Liability; Section 10 – Confidentiality; Section 11 – Proprietary Rights; Data; Feedback; Section 13 – Force Majeure; Delays Caused by Customer; Section 14 – Disputes; and Section 15 – General.

15.12. Entire Agreement. This Agreement, including all Exhibits, Addenda, and Proposals, constitutes the entire agreement of the Parties regarding the subject matter hereto, and supersedes all previous agreements, proposals, and understandings, whether written or oral, relating to this subject matter. This Agreement may be executed in multiple counterparts, and will have the same legal force and effect as if the Parties had executed it as a single document. The Parties may sign in writing or by electronic signature. An electronic signature, facsimile copy, or computer image of a signature, will be treated, and will have the same effect as an original signature, and will have the same effect, as an original signed copy of this document. This Agreement may be amended or modified only by a written instrument signed by authorized representatives of both Parties. The preprinted terms and conditions found on any Customer purchase order, acknowledgment, or other form will not be considered an amendment or modification or part of this Agreement, even if a representative of each Party signs such document.

The Parties hereby enter into this MCA as of the Effective Date.

Motorola Solutions, Inc.

Customer: _____

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Software License Addendum

This Software License Addendum (this “**SLA**”) is subject to, and governed by, the terms of the Motorola Solutions Customer Agreement (“**MCA**”) to which it is attached. Capitalized terms used in this SLA, but not defined herein, will have the meanings set forth in the MCA.

Section 1. Addendum. This SLA governs Customer’s use of Licensed Software (and, if set forth in a Proposal, related Services) and Subscription Software from Motorola, as applicable, and is an integral part of the Parties’ Agreement.

Section 2. Licensed Software License and Restrictions.

2.1. Licensed Software License. Subject to Customer’s and its Authorized Users’ compliance with the Agreement (including payment terms), Motorola hereby grants Customer and its Authorized Users a limited, non-transferable, non-sublicensable, and non-exclusive license to use the Licensed Software identified in a Proposal, in object code form only, and the associated Documentation, solely in connection with the Equipment provided by Motorola or authorized Customer-Provided Equipment (as applicable, the “**Designated Products**”) and solely for Customer’s internal business purposes. Unless otherwise stated in an Addendum or the Proposal, the foregoing license grant will be limited to the number of licenses set forth in the applicable Proposal and will continue for the life of the applicable Designated Product. Except as otherwise permitted in an applicable Addendum or Proposal, Customer may install, access, and use Licensed Software only in Customer’s owned or controlled facilities, including any authorized mobile sites; provided, however, that Authorized Users using authorized mobile or handheld devices may also log into and access the Licensed Software remotely from any location.

2.2. Subscription License Model. If the Parties mutually agree that any Licensed Software purchased under this Agreement will be replaced with or upgraded to Subscription Software, then upon such time which the Parties execute the applicable Change Order or Proposal, the licenses granted under this **Section 2 Licensed Software License and Restrictions** will automatically terminate, and such Subscription Software will be governed by the terms of **Section 3 Subscription Software License and Restrictions**.

2.3. Customer Restrictions. Customers and Authorized Users will comply with the applicable Documentation in connection with their use of the Products. Customer will not and will not allow others, including the Authorized Users, to: (a) make the Licensed Software available for use by unauthorized third parties, including via a commercial rental or sharing arrangement; (b) reverse engineer, disassemble, or reprogram the Licensed Software or any portion thereof to a human-readable form; (c) modify, create derivative works of, or merge the Licensed Software with other software or equipment; (d) copy, reproduce, distribute, lend, lease, or transfer the Licensed Software or Documentation for or to any third party without the prior express written permission of Motorola; (e) take any action that would cause the Licensed Software or Documentation to be placed in the public domain; (f) use the Licensed Software to compete with Motorola; or (g) remove, alter, or obscure, any copyright or other notice.

2.4. Copies. Customer may make one (1) copy of the Licensed Software solely for archival, back-up, or disaster recovery purposes during the term of the applicable Licensed Software license. Customer may make as many copies of the Documentation reasonably required for the internal use of the Licensed Software during such Licensed Software’s license term. Unless otherwise authorized by Motorola in writing, Customer will not, and will not enable or allow any third party to: (a) install a licensed copy of the Licensed Software on more than one (1) unit of a Designated Product; or (b) copy onto or transfer Licensed Software installed in a unit of a Designated Product onto another device. Customer may temporarily transfer Licensed Software installed on a

Designated Product to another device if the Designated Product is inoperable or malfunctioning, if Customer provides written notice to Motorola of the temporary transfer and identifies the device on which the Licensed is transferred. Temporary transfer of the Licensed Software to another device must be discontinued when the original Designated Product is returned to operation and the Licensed Software must be removed from the other device. Customer must provide prompt written notice to Motorola at the time the temporary transfer is discontinued.

- 2.5. Resale of Equipment.** Equipment contains embedded Licensed Software. If Customer desires to sell its used Equipment to a third party, Customer must first receive prior written authorization from Motorola, which will not be unreasonably denied, and obtain written acceptance of the applicable Licensed Software license terms, including the obligation to pay relevant license fees, from such third party.

Section 3. Subscription Software License and Restrictions.

- 3.1. Subscription Software License.** Subject to Customer's and its Authorized Users' compliance with the Agreement, including payment terms, Motorola hereby grants Customer and its Authorized Users a limited, non-transferable, non-sublicensable, and non-exclusive license to use the Subscription Software identified in a Proposal, and the associated Documentation, solely for Customer's internal business purposes. The foregoing license grant will be limited to use in the territory and to the number of licenses set forth in a Proposal (if applicable), and will continue for the applicable Subscription Term. Customer may access, and use the Subscription Software only in Customer's owned or controlled facilities, including any authorized mobile sites; provided, however, that Authorized Users using authorized mobile or handheld devices may also log into and access the Subscription Software remotely from any location. No custom development work will be performed under this Addendum.
- 3.2. Customer Restrictions.** Customers and Authorized Users will comply with the applicable Documentation and the copyright laws of the United States and all other relevant jurisdictions (including the copyright laws where Customer uses the Subscription Software) in connection with their use of the Subscription Software. Customer will not, and will not allow others including the Authorized Users, to make the Subscription Software available for use by unauthorized third parties, including via a commercial rental or sharing arrangement; reverse engineer, disassemble, or reprogram software used to provide the Subscription Software or any portion thereof to a human-readable form; modify, create derivative works of, or merge the Subscription Software or software used to provide the Subscription Software with other software; copy, reproduce, distribute, lend, or lease the Subscription Software or Documentation for or to any third party; take any action that would cause the Subscription Software, software used to provide the Subscription Software, or Documentation to be placed in the public domain; use the Subscription Software to compete with Motorola; remove, alter, or obscure, any copyright or other notice; share user credentials (including among Authorized Users); use the Subscription Software to store or transmit malicious code; or attempt to gain unauthorized access to the Subscription Software or its related systems or networks.
- 3.3. User Credentials.** If applicable, Motorola will provide Customer with administrative user credentials for the Subscription Software, and Customer will ensure such administrative user credentials are accessed and used only by Customer's employees with training on their proper use. Customer will protect, and will cause its Authorized Users to protect, the confidentiality and security of all user credentials, including any administrative user credentials, and maintain user credential validity, including by updating passwords. Customer will be liable for any use of the Subscription Software through such user credential (including through any administrative user credentials), including any changes made to the Subscription Software or issues or user impact arising therefrom. To the extent Motorola provides Services to Customer in order to help resolve

issues resulting from changes made to the Subscription Software through user credentials, including through any administrative user credentials, or issues otherwise created by Authorized Users, such Services will be billed to Customer on a time and materials basis, and Customer will pay all invoices in accordance with the payment terms of the MCA.

Section 4. Software Systems - Applicable Terms and Conditions

4.1. On-Premise Software System. If Customer purchases an “on-premises Software System,” where Licensed Software is installed at Customer Sites or on Customer-Provided Equipment, then, unless otherwise specified in writing that any software is being purchased as Subscription Software, the Licensed Software is subject to Section 2 of the SLA.

4.1.1. CAD and Records Products. The terms set forth in this Section 4.1.1. apply in the event Customer purchases any Computer Aided Dispatch (“CAD”) or Records Products under the Agreement.

4.1.1.1. Support Required. Customer acknowledges and agrees that the licenses granted by Motorola under this SLA to CAD and Records Products for on-premises Software Systems are conditioned upon Customer purchasing Maintenance and Support Services for such Products during the term of the applicable license. If at any time during the term of any such license, Customer fails to purchase associated Maintenance and Support Services (or pay the fees for such Services), Motorola will have the right to terminate or suspend the software licenses for CAD and Record Products.

4.1.1.2. CJIS Security Policy. Motorola agrees to support Customer’s obligation to comply with the Federal Bureau of Investigation Criminal Justice Information Services (“CJIS”) Security Policy and will comply with the terms of the CJIS Security Addendum for the term of the Addendum or Proposal for the applicable Product. Customer hereby consents to Motorola screened personnel serving as the “escort” within the meaning of CJIS Security Policy for unscreened Motorola personnel that require access to unencrypted Criminal Justice Information for purposes of Product support and development.

4.2. On-Premise Software System as a Service. If Customer purchases an “on-premises Software System as a service,” where software Products are installed at Customer Sites or on Customer-Provided Equipment, and generally licensed on a subscription basis (i.e, as Subscription Software), then such Subscription Software is subject to Section 3 of the SLA. The firmware preinstalled on Equipment included with an on-premises Software System as a service purchase, and any Microsoft operating system Licensed Software are subject to Section 2 of the SLA.

4.2.1. Transition to Subscription License Model. If the Parties mutually agree that any on-premises Subscription Software purchased under this SLA as part of an “on-premises Software System as a service” solution will be replaced with or upgraded to Subscription Software hosted in a data center, then upon such time the Parties execute the applicable agreement, (a) the licenses granted to such on-premises Subscription Software under this SLA will automatically terminate, (b) Customer and its Authorized Users will cease use of the applicable on-premises copies of Subscription Software, and (c) the replacement hosted Subscription Software provided hereunder will be governed by the terms of **Section 4.3 Cloud Hosted Software System**.

4.2.2. Transition Fee. Motorola will not charge additional Fees for Services related to the transition to hosted Subscription Software, as described in **Section 4.2.1 – Transition to Subscription License Model**. Notwithstanding the foregoing, subscription Fees may be greater than Fees paid by Customer for on-premises Subscription Software.

4.2.3. Software Decommissioning. Upon (a) transition of the on-premises Software System as a service to Subscription Software hosted in a data center or (b) any termination of the Subscription Software license for the on-premises Software System as a service, Motorola will have the right to enter Customer Sites and decommission the applicable on-premises Subscription Software that is installed at Customer's Site or on Customer-Provided Equipment. For clarity, Customer will retain the right to use Licensed Software that is firmware incorporated into Equipment purchased by Customer from Motorola and any Microsoft operating system Licensed Software.

4.3. Cloud Hosted Software System. If Customer purchases a "cloud hosted Software System," where the applicable software is hosted in a data center and provided to Customer as a service (i.e., as hosted Subscription Software), then such Subscription Software is subject to Section 3 of the SLA.

4.4. Additional Cloud Terms. The terms set forth in this **Section 4.4 – Additional Cloud Terms** apply in the event Customer purchases any cloud-hosted software Products.

4.4.1. Data Storage. Motorola will determine, in its sole discretion, the location of the stored content for cloud hosted software Products. All data, replications, and backups will be stored at a location in the United States for Customers in the United States.

4.4.2. Data Retrieval. Cloud hosted software Products will leverage different types of storage to optimize software, as determined in Motorola's sole discretion. For multimedia data, such as videos, pictures, audio files, Motorola will, in its sole discretion, determine the type of storage medium used to store the content. The type of storage and medium selected by Motorola will determine the data retrieval speed. Access to content in archival storage may take up to twenty-four (24) hours to be viewable.

4.4.3. Maintenance. Scheduled maintenance of cloud-hosted software Products will be performed periodically. Motorola will make commercially reasonable efforts to notify customers one (1) week in advance of any such maintenance. Unscheduled and emergency maintenance may be required from time to time. Motorola will make commercially reasonable efforts to notify customers of any unscheduled or emergency maintenance twenty-four (24) hours in advance.

Section 5. Term.

5.1. Term. The term of this SLA (the "**SLA Term**") will commence upon the Effective Date of the MCA.

5.2. Termination - Licensed Software License. Notwithstanding the termination provisions of the MCA, Motorola may terminate this SLA (and any Agreements hereunder) immediately upon notice to Customer if Customer breaches **Section 2 – Licensed Software License and Restrictions** of this SLA, or any other provision related to Licensed Software license scope or restrictions set forth in a Proposal, EULA, or other applicable Addendum. Upon termination or expiration of the SLA Term, all Motorola obligations under this SLA (including with respect to Equipment and Licensed Software delivered hereunder) will terminate. If Customer desires to purchase additional Services in connection with such Equipment or Licensed Software, Customer may enter into a separate Addendum with Motorola, governing such Services.

5.3. Termination - Subscription Software License. Notwithstanding the termination provisions of the MCA, Motorola may terminate this SLA, or suspend delivery of Subscription Software or Services, immediately upon notice to Customer if (a) Customer breaches **Section 3 – Subscription Software License and Restrictions** of this SLA, or any other provision related to Subscription Software license scope or restrictions set forth therein, or (b) it determines that Customer's use of the Subscription Software poses, or may pose, a security or other risk or adverse impact to any

Subscription Software, Motorola, Motorola's systems, or any third party (including other Motorola customers).

5.4. Customer acknowledges that Motorola made a considerable investment of resources in the development, marketing, and distribution of the Licensed Software, Subscription Software, and Documentation, and that Customer's breach of the SLA will result in irreparable harm to Motorola for which monetary damages would be inadequate. If Customer breaches this SLA, in addition to termination, Motorola will be entitled to all available remedies at law or in equity (including immediate injunctive relief).

5.5. Applicable End User Terms. Additional license terms apply to third-party software included in certain software Products which are available online at www.motorolasolutions.com/legal-flow-downs. Customer will comply, and ensure its Authorized Users comply, with all such additional license terms.

Section 6. Copyright Notices. The existence of a copyright notice on any Licensed Software will not be construed as an admission or presumption of publication of the Licensed Software or public disclosure of any trade secrets associated with the Licensed Software.

Section 7. Survival. The following provisions will survive the expiration or termination of this SLA for any reason: Section 2 – Licensed Software License and Restrictions; Section 3 -- Subscription Software License and Restrictions; Section 4 -- Software Systems -- Applicable Terms and Conditions; Section 5 – Term; Section 7 – Survival.

Mobile Video and Vigilant Addendum

This Mobile Video and Vigilant Addendum (this “**MVVA**”) is subject to, and governed by, the terms of the Motorola Solutions Customer Agreement (“**MCA**”) to which it is attached. Capitalized terms used in this MVVA, but not defined herein, will have the meanings set forth in the MCA.

Section 1. Addendum. This MVVA governs Customer’s purchase of (a) any Motorola mobile video Products, including participation in Motorola’s Video-as-a-Service Program (“**VaaS Program**”), and (b) Motorola’s Vigilant automated license plate recognition software and hardware Products (“**LPR Products**”). This MVVA will control with respect to conflicting or ambiguous terms in the MCA or any other applicable Addendum, but only as applicable to the Mobile Video System or other Products purchased under this MVVA.

Section 2. Definitions.

“**Mobile Video System**” is a solution that includes at least one mobile video Product and requires Integration Services to deploy such mobile video Product or the associated evidence management Product at a Customer Site.

Camera License Key (“CLK”) means an electronic key that will permit each camera (one CLK per camera) to be used with Vigilant CarDetector and/or Subscription Software

Commercial Booking Images refers to booking images collected by commercial sources and available on Vigilant VehicleManager with a paid subscription.

Commercial Data means both Commercial Booking Images and Commercial LPR Data.

Commercial LPR Data refers to LPR data collected by private sources and available on Vigilant VehicleManager with a paid subscription.

License Plate Recognition (“LPR”) refers to the process of utilizing cameras, either stationary or mounted on moving vehicles, to capture and interpret images of vehicle license plates.

Section 3. Evidence Management Systems; Applicable Terms and Conditions.

3.1. On-Premise Evidence Management. If Customer purchases a Mobile Video System where Equipment and Licensed Software for evidence management is installed at Customer Sites (an “**On-Premises Evidence Management System**”), then, unless the Proposal specifies that any software is being purchased as Subscription Software, any (i) Equipment and (ii) Licensed Software installed at Customer Sites or on Customer-Provided Equipment purchased in connection with the On-Premises Evidence Management System is subject to the SLA. On-Premises Evidence Management Systems described in this Section qualify for the System Warranty as described in **Section 5 – On-Premises Evidence Management System Warranty** (the “**System Warranty**”).

3.2. Cloud Hosted Evidence Management. If Customer purchases a Mobile Video System where the software for evidence management is hosted in a data center and provided to Customer as a service (“**Cloud Hosted Evidence Management System**”), then such software is subject to the SLA. Any Equipment purchased in connection with the Cloud Hosted Evidence Management System is subject to the MCA. System Warranty does not apply to Cloud Hosted Evidence Management Systems. System completion is determined in accordance with the provisions of **Section 12 –System Completion** below.

3.3. Services. Any Integration Services or Maintenance and Support Services purchased in connection with, or included as a part of, a Mobile Video System are subject to the MCA, and as described in the applicable Addendum.

Section 4. Payment. Customer will pay invoices for the Products and Services covered by this MVVA in accordance with the invoice payment terms set forth in the MCA. Fees for Mobile Video Systems will be invoiced as of the System Completion Date, unless another payment process or schedule is set forth in the Proposal.

Section 5. On-Premises Evidence Management System Warranty. Subject to the disclaimers in the MCA and any other applicable Addenda, Motorola represents and warrants that, on the System Completion Date (as defined below) for an On-Premises Evidence Management System described in **Section 3.1 – On-Premises Evidence Management** (a) such On-Premises Evidence Management System will perform in accordance with the descriptions in the applicable Proposal in all material respects, and (b) if Customer has purchased any Equipment or Motorola Licensed Software (but, for clarity, excluding Subscription Software) as part of such On-Premises Evidence Management System, the warranty period applicable to such Equipment and Motorola Licensed Software will continue for a period of one (1) year commencing upon the System Completion Date for the On-Premises Evidence Management System that includes such Products, or on the applicable Product Completion Date, if earlier.

Section 6. Additional Software and Video Terms and Conditions.

6.1. Unlimited Storage. Storage shall be specifically described in Proposal. “Unlimited Storage” related to Customer’s purchase of a Cloud Hosted Evidence Management system means storage of all data captured using Equipment sold under this MVA, provided that (1) video recordings are recorded in an event-based setting where users are not recording an entire shift under one video footage and (2) Customer’s data retention policies and practices do not result in the retention of data beyond the statutory minimums set forth by the State in which the Customer resides. In the event Customer does not comply with the preceding clauses (1) and (2), Motorola shall have the right to charge Customer for such excess data storage at the prevailing rates. Motorola also has the right to place any data that has not been accessed for a consecutive six (6) month period into archival storage, retrieval of which may take up to twenty-four (24) hours from any access request.

6.2. Applicable End User Terms. Described in Section 5.6 of the SLA.

6.3. License Plate Recognition Data Ownership and Retention. Motorola retains all title and rights to Commercial LPR Data and Commercial Booking Images. Customer shall not utilize Commercial LPR Data or Commercial Booking Images on the behalf of other local, state or Federal law enforcement agencies (“LEAs”). LPR data and where applicable, booking images, collected by the License plate recognition (“LPR”) data collected by Customer is considered Customer Data (as defined in the MCA) and is therefore subject to the Customer’s own retention policy. LPR data and/or booking images that has reached the end of the retention period set by the Customer in ClientPortal or VehicleManager will be deleted in accordance thereof. Customer retains all rights to LPR data and booking images collected by Customer.

6.3.1 Data Sharing. Customer, at its option, may share its LPR data with other similarly situated LEAs which contract with Motorola to access Vigilant VehicleManager by selecting this option within Vigilant VehicleManager. Other similarly situated LEAs may similarly opt to share their LPR data with Customer using Vigilant VehicleManager. Such LPR data generated by other LEAs is considered Third-Party Data (as defined in the MCA), is governed by the retention policy of the respective LEA, and shall be used by Customer only in connection with its use of Vigilant VehicleManager.

6.3.2. Only individuals who are agents and/or sworn officers of Customer and who are authorized by Customer to access Vigilant VehicleManager on behalf of Customer through login credentials provided by Customer (“**User Eligibility Requirements**”) may access Vigilant

VehicleManager. Motorola in its sole discretion may deny access to Vigilant VehicleManager to any individual based on such person's failure to meet the User Eligibility Requirements. Customer will ensure no user logins are provided to agents or officers of other local, state, or Federal LEAs without the express written consent of Motorola. Customer will be responsible for all individuals' access to, and use of, Vigilant VehicleManager through use of Customer login credentials, including ensuring their compliance with this Agreement. Customer shall notify Motorola immediately if Customer believes the password of any of its Users has, or may have, been obtained or used by any unauthorized person(s). In addition, Customer must notify Motorola immediately if it becomes aware of any other breach or attempted breach of the security of any of its Users' accounts.

6.3.3 LEA Customers. If Customer is an LEA, other similarly situated LEAs that collect their own LPR data and booking images may opt to share such data with Customer using VehicleManager.

6.3.4. Non-LEA Customers. If Customer is a non-LEA Customer, other similarly situated ClientPortal customers that collect their own LPR data may opt to share such data with Customer using ClientPortal. Such LPR data generated by other ClientPortal customers is considered Third-Party Data (as defined in the MCA), is governed by the retention policy of the respective ClientPortal customer, and shall be used by Customer only in connection with its use of ClientPortal. Third-party LPR data that has reached its expiration date will be deleted from ClientPortal in accordance with the retention terms of the sharing entity.

6.4. Commercial Data Access. If Customer purchases a subscription to Commercial Data, then Customer shall execute and agree to the terms of Motorola's standard Data License Addendum, a copy of which is available upon request.

6.5. API Support. Described in the MCA.

6.6. Support of Downloaded Clients. Described in the MCA.

6.7. CJIS Security Policy. Described in the MCA.

Section 7. VaaS Program Terms. All hardware provided by Motorola to Customer under the VaaS Program will be considered Equipment, as defined in the MCA and constitutes a purchase of Equipment subject to the terms and conditions contained therein. In addition, the following terms and conditions apply to any Equipment purchased under the VaaS Program:

7.1. Technology Refresh. Body cameras and associated batteries purchased under the VaaS Program ("**Body Cameras**") may be eligible for a technology refresh as described in the Proposal. If included in the Proposal, and in the event the Body Camera is eligible for replacement applicable under this **Section 7.1 – Technology Refresh**, Customer must return the existing Body Camera to Motorola in working condition. The corresponding replacement Body Camera will be the then-current model of the Body Camera at the same tier as the Body Camera that is returned to Motorola. For clarity, any other Equipment received by Customer as part of the VaaS Program, other than Body Cameras, or associated batteries (if specified in the Proposal) will not be eligible for a technology refresh hereunder.

7.2. No-Fault Warranty. If specified in the Proposal, and subject to the disclaimers set forth in the Agreement, upon delivery of Equipment purchased as part of the VaaS Program, Motorola will provide a No-fault Warranty to Customer for such Equipment that extends until the end of the Commitment Term (as defined below) applicable to such Equipment; except that the No-fault Warranty will not apply to: (i) any Equipment with intentionally altered or removed serial numbers, (ii) any other damages disclaimed under the MCA, or (iii) any Equipment that Motorola determines

was changed, modified, or repaired by Customer or any third party. The “**No-fault Warranty**” means that Motorola will repair or replace any Equipment components or parts that render the applicable Equipment unable to perform its intended purpose. With respect to any batteries in Body Cameras, a battery will be considered faulty and covered under this No-fault Warranty if it falls below sixty percent (60%) of rated capacity.

7.3. Commitment Term. Customer accepts that following the delivery of any Equipment under the VaaS Program, Customer commits to a five (5) year subscription term for such Equipment at the rate provided in the Proposal (the “**Initial Commitment Term**”). If Customer, for any reason, terminates any of its obligations to Motorola prior to expiration of the applicable Commitment Term (as defined below), Customer will be subject to the payments described in **Section 11.2 – Termination** hereunder.

Section 8. Additional Devices. Any additional Equipment, including any accessory items, ordered by Customer after Customers’ initial purchase of Equipment hereunder may be subject to an incremental increase in Fees. In the event Customer orders additional Equipment under the VaaS Program within the ninety (90) days immediately following its initial purchase, such Equipment will be included in and subject to the Initial Commitment Term. Any additional Equipment purchased under the VaaS Program subsequent to such ninety (90) day period, will commence an additional subscription term commitment for such Equipment of five (5) years (a “**Subsequent Commitment Term**”) with respect to the monthly Fee associated with such additional Equipment. For purposes of this Addendum, the Initial Commitment Term and each Subsequent Commitment Term are each also referred to herein as a “**Commitment Term**”.

Section 9. Included Subscription Software.

9.1 VideoManager EL. Subject to **Section 11.1 – VaaS Term**, if the Equipment purchased under the VaaS Program provides Customer with a subscription to the Cloud Hosted Evidence Management System during the VaaS Term (as defined below), use of the Cloud Hosted Evidence Management System is subject to the MCA and SLA. Customer’s subscription will include unlimited users, Unlimited Storage and unlimited sharing, provided any media or data uploaded to the Cloud Hosted Evidence Management System is done using Motorola Equipment actively enrolled in the VaaS Program. Following expiration of the applicable Commitment Term, Customer’s continued use of expired Equipment with the Cloud Hosted Evidence Management System is subject to Customer’s purchase of additional access at Motorola’s prevailing rates, or Motorola may disconnect connectivity of any expired Equipment to the Cloud Hosted Evidence Management System.

9.2 CommandCentral. If specified and included in the Proposal, for each applicable Body Camera, in-car system or integrated system purchased, Customer will receive one user license for Motorola CommandCentral (CC), which provides access to CC Community, CC Capture, CC Vault and CC Records. Additional CC licenses may be purchased for an additional fee.

9.3 VideoManager EX: Subject to **Section 11.1 – VaaS Term**, if specified in the Proposal, Equipment purchased under the VaaS Program provides Customer with a single subscription to Video Manager EX during the VaaS Term (as defined below), the use of which is subject to the MCA and SLA. Following expiration of the applicable Commitment Term, Customer must purchase additional access to VideoManager EX, at Motorola’s prevailing rates, to continue using expired Equipment with the VideoManager EX, or Motorola may disconnect connectivity of any expired Equipment.

9.4. Vigilant VehicleManager or Vigilant ClientPortal. The VaaS Program provides Customer with a subscription to Vigilant VehicleManager or Vigilant ClientPortal, as specified in the

Proposal, during the VaaS Term (as defined below). Following expiration of the applicable Commitment Term, if Customer desires to continue use of expired Equipment with the Vigilant VehicleManager or Vigilant ClientPortal, Customer must purchase additional access to Vigilant VehicleManager or Vigilant ClientPortal based on Motorola's prevailing rates, or Motorola may disconnect connectivity of any expired Equipment to such software.

9.4.1. Access. Use and access to VehicleManager is strictly restricted to Law Enforcement Agencies ("LEAs") and their Authorized Users. Non-LEAs and their Authorized Users may purchase/access Client Portal.

9.5. CarDetector. Customer Customer may purchase Vigilant CarDetector which is Subscription Software. For Customers subscribing to CarDetector, Customer is required to obtain a CLK for each Motorola-approved camera which uses CarDetector. A CLK can be obtained by Customer by going to Motorola's company support website and completing the online request form to Vigilant technical support staff.

Section 10. VaaS Program Payment.

10.1 Mobile Video System: Unless otherwise provided in a Proposal (and notwithstanding the provisions of the MCA), Customer will prepay a subscription Fee quarterly (each a "**Subscription Quarter**"), as set forth in a Proposal. If Customer orders any additional Product(s) under the VaaS Program subsequent to the initial purchase by Customer, Fees for such additional Product will be added to the quarterly subscription Fee, and will be payable on the same Fee payment schedule as the initial Product purchased under the VaaS Program; provided, however, that for the first Subscription Quarter during which such additional Product is purchased, the subscription Fee for the applicable additional Product will be prorated based on the applicable number of days remaining in the such initial Subscription Quarter.

10.2 LPR System: Unless otherwise provided in a Proposal (and notwithstanding the provisions of the MCA), Customer will prepay a subscription Fee yearly (each a "Subscription Year"), as set forth in a Proposal. If Customer orders any additional LPR Product(s) under the VaaS Program subsequent to Customer's initial purchase, the Fees for the additional LPR Product will be added to the yearly subscription Fee and will be payable on the same Fee payment schedule as the initial LPR Products purchased by the Customer; provided, however, that for the first Subscription Year during which such additional LPR Product(s) is purchased, the subscription Fee for the applicable additional LPR Product(s) will be prorated based on the applicable number of days remaining in such initial Subscription Year.

Section 11. VaaS Program Term and Termination.

11.1 VaaS Term. Customer's participation in the VaaS Program will commence upon the System Completion Date under this MVA, and will continue through the end of the final Commitment Term hereunder ("the "**VaaS Term**"). Following the end of any Commitment Term, Customer's access to the Cloud Hosted Evidence Management System with respect to the Equipment purchased relative to that Commitment Term will expire, and Customer must download or transfer all Customer Data associated with the applicable Equipment within thirty (30) days following expiration unless Customer purchases extended access to the Cloud Hosted Evidence Management System from Motorola at the prevailing rates. Motorola has no obligation to retain Customer Data for expired Equipment beyond thirty (30) days following expiration of the applicable Commitment Term. For example, if Customer purchases 100 devices on January 1 of Year 1 of the VaaS Term or the Initial Commitment Term, and then 100 additional devices on January 1 of Year 3, on December 31 of Year 5 (i.e., the conclusion of the Initial Commitment Term), Customer's access to the Cloud Hosted Evidence Management System with respect to

the first 100 devices will be discontinued, and Customer must purchase extended storage or transfer all Customer Data associated with the first 100 devices within thirty (30) days of expiration of the Initial Commitment Term. In the foregoing example, the Cloud Hosted Evidence Management System access and data storage for the second 100 devices purchase will extend until December 31 of Year 7.

11.2 Termination. The termination provisions applicable to the VaaS Program will be those set forth in the MCA and SLA, as applicable. If Customer's participation in the VaaS Program is terminated for any reason prior to the end of the Initial Commitment Term or any Subsequent Commitment Term, Customer will pay the prorated remainder of the aggregate Equipment list price (prevailing as of the time of delivery). This is calculated by multiplying the list price of all Equipment purchased under the VaaS Program by the percentage resulting from dividing the number of months remaining in the Commitment Term applicable to such Equipment by sixty (60). In the event Customer purchased Equipment on multiple dates, resulting in separate Commitment Terms, the preceding calculation will be made relative to the applicable Commitment Term for each Equipment order.

11.3 Post Termination Subscription Software Access. Upon completion of the VaaS Term, Customer may elect to purchase additional CLKs, at then current rates, for continued Vigilant CarDetector and/or Subscription Software access. If applicable, additional network costs, at then current rates, may apply. Any continued Software Subscription access shall continue to be governed by the MCA and SLA.

Section 12. System Completion. Any Mobile Video System sold hereunder will be deemed completed upon Customer's (or the applicable Authorized User's) Beneficial Use of the applicable Mobile Video System (the "**System Completion Date**"). Customer will not unreasonably delay Beneficial Use, and in any event, the Parties agree that Beneficial Use will be deemed to have occurred thirty (30) days after functional demonstration. As used in this Section, "**Beneficial Use**" means use by Customer or at least one (1) Authorized User of the material features and functionalities of Mobile Video System, in material conformance with Product descriptions in the applicable Proposal. Any additional Equipment sold in connection with the initial Mobile Video System shall be deemed delivered in accordance with the terms of the MCA. Any additional Subscription Software purchased under the VaaS Program will be deemed delivered upon Customer's receipt of credentials required for access to the Cloud Hosted Evidence Management System or upon Motorola otherwise providing access to the Cloud Hosted Evidence Management System. This Section applies to Products purchased under the MVA notwithstanding any delivery provisions of the Agreement, and this Section will control over such other delivery provisions to the extent of a conflict.

Section 13. Additional Cloud Terms. The terms set forth in Section 4.4 Additional Cloud Terms of the SLA apply in the event Customer purchases any cloud hosted software Products, including a Cloud Hosted Evidence Management System.

Section 14. Survival. The following provisions will survive the expiration or termination of this MVVA for any reason: Section 1 – Addendum; 3 – Evidence Management Systems; Applicable Terms and Conditions; Section 4 – Payment; Section 6.2 – Applicable End User Terms; Section 9.1 – VideoManager EL Section 11 – VaaS Program Term and Termination; Section 14 – Survival.

MAINTENANCE, SUPPORT AND LIFECYCLE MANAGEMENT ADDENDUM

This Maintenance, Support and Lifecycle Management Addendum (this “**MSLMA**”) is subject to, and governed by, the terms of the Motorola Solutions Customer Agreement (“MCA”) to which it is attached. Capitalized terms used in this MSLMA, but not defined herein, will have the meanings set forth in the MCA.

Section 1. Addendum. This MSLMA governs Customer’s purchase of Maintenance, Support and Lifecycle Management (as defined below) services (and, if set forth in an Proposal related Services) from Motorola and will form part of the Parties’ Agreement. This MSMLA will control with respect to conflicting terms in the MCA or any other applicable Addendum, but only as applicable to the Maintenance, Support and Lifecycle Management services purchased under this MSMLA and not with respect to other Products and Services.

Section 2. Scope

Motorola will provide break/fix maintenance, technical support, or other Services (such as software integration Services) (“Maintenance and Support Services”) and/or upgrade services (“Lifecycle Management”) as further described in the applicable Proposal.

Section 3. Terms and conditions

3.1 Maintenance and Support services

3.1.1 Purchase Order Acceptance. Purchase orders for additional, continued, or expanded maintenance and software support, during the Warranty Period or after the Warranty Period, become binding only when accepted in writing by Motorola.

3.1.2 Start Date. The “Start Date” for Maintenance and Support Services will be indicated in the applicable Proposal.

3.1.3 Auto Renewal. Unless the applicable Proposal specifically states a termination date or one Party notifies the other in writing of its intention to discontinue the Maintenance and Support Services, this Agreement will renew for an additional one (1) year term on every anniversary of the Start Date. At the anniversary date, Motorola may adjust the price of the Services to reflect the renewal rate.

3.1.4 Termination. Written notice of intent to terminate must be provided thirty (30) days or more prior to the anniversary date. If Motorola provides Services after the termination or expiration of this MSLMA, the terms and conditions in effect at the time of termination or expiration will apply to those Services and Customer agrees to pay for those services on a time and materials basis at Motorola’s then effective hourly rates. This provision survives the expiration or termination of the Agreement and applies notwithstanding any contrary provision.

3.1.5 Equipment Definition. For maintenance and support services, Equipment will be defined to mean the hardware specified in the applicable Proposal.

3.1.6 Additional Hardware. If Customer purchases additional hardware from Motorola that becomes part of the Communications System, the additional hardware may be added to this MSLMA and will be billed at the applicable rates after the warranty period for that additional equipment expires. Such hardware will be included in the definition of Equipment.

3.1.7 Maintenance. Equipment will be maintained at levels set forth in the manufacturer's product manuals and routine procedures that are prescribed by Motorola will be followed. Motorola parts or parts of equal quality will be used for Equipment maintenance.

3.1.8 Equipment Condition. All Equipment must be in good working order on the Start Date or when additional equipment is added to the MSLMA. Upon reasonable request by Motorola, Customer will provide a complete serial and model number list of the Equipment. Customer must promptly notify Motorola in writing when any Equipment is lost, damaged, stolen or taken out of service. Customer's obligation to pay maintenance and support fees for this Equipment will terminate at the end of the month in which Motorola receives the written notice. If Equipment cannot, in Motorola's reasonable opinion, be properly or economically maintained for any reason, Motorola may modify the scope of Services related to that Equipment; remove that Equipment from the Agreement; or increase the price to maintain that Equipment.

3.1.9 Equipment Failure. Customer must promptly notify Motorola of any Equipment failure. Motorola will respond to Customer's notification in a manner consistent with the level of Service purchased as indicated in this MSLMA and applicable Proposal.

3.1.10 Intrinsically Safe. Customer must specifically identify any Equipment that is labeled intrinsically safe for use in hazardous environments.

3.1.11 Excluded Services.

a) Service excludes 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.

b) Unless specifically included in this MSLMA or the applicable Proposal, Service excludes items that are consumed in the normal operation of the Equipment, such as batteries or magnetic tapes.; upgrading or reprogramming Equipment; accessories, belt clips, battery chargers, custom or special products, modified units, or software; 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.

3.1.12 Time And Place. Service will be provided at the location specified in this MSLMA and/or the applicable Proposal. When Motorola performs maintenance, support, or installation at Customer's location, Customer will provide Motorola, at no charge, a non-hazardous work environment with adequate shelter, heat, light, and power and with full and free access to the Equipment. Waivers of liability from Motorola or its subcontractors will not be imposed as a site access requirement. Customer will provide all information pertaining to the hardware and software elements of any system with which the Equipment is interfacing so that Motorola may perform its Services. Unless otherwise stated in this MSLMA or applicable Proposal, the hours of Service will be 8:30 a.m. to 4:30 p.m., local time, excluding weekends and holidays. Unless otherwise stated in this MSLMA or applicable Proposal, the price for the Services exclude any charges or expenses associated with helicopter or other unusual access requirements; if these charges or expenses are reasonably incurred by Motorola in rendering the Services, Customer agrees to reimburse Motorola for those charges and expenses.

3.1.13 Customer Contact. Customer will provide Motorola with designated points of contact (list

of names and phone numbers) that will be available twenty-four (24) hours per day, seven (7) days per week, and an escalation procedure to enable Customer's personnel to maintain contact, as needed, with Motorola.

3.1.14 Warranty. Motorola warrants that its Maintenance and Support Services under this section will be free of defects in materials and workmanship for a period of ninety (90) days from the date the performance of the Services are completed. In the event of a breach of this warranty, Customer's sole remedy is to require Motorola to re-perform the non-conforming Service or to refund, on a pro-rata basis, the fees paid for the non-conforming Service. MOTOROLA DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

3.2 Lifecycle Management Services

3.2.1 The License terms included in the MCA and its SLA Addendum apply to any Motorola Licensed Software provided as part of the Lifecycle Management transactions.

3.2.2 The term of this MSLMA is 5 years, commencing on , 202 . The Lifecycle Management Price for the 5 years of services is \$436,274, excluding applicable sales or use taxes but including discounts as more fully set forth in the pricing pages. Because the Lifecycle Management is a subscription service as more fully described in the applicable Proposal, payment from Customer is due in advance and will not be in accordance with any Payment Milestone Schedule.

3.2.3 The Communications System upgrade will be scheduled during the subscription period and will be performed when Motorola's upgrade operation resources are available. Motorola may substitute any of the promised Equipment or Licensed Software so long as the substitute is equivalent or superior to the initially promised Equipment or Licensed Software.

3.2.4 Acceptance of a Lifecycle Management transaction occurs when the Equipment (if any) and Licensed Software are delivered, in accordance with the MCA, and the Lifecycle Management services are fully performed.

3.2.5 The Warranty Period for any Equipment or Licensed Software provided under a Lifecycle Management transaction will commence upon shipment and is for a period of ninety (90) days. The ninety (90) day warranty for Lifecycle Management services is set forth in the applicable Proposal.

3.2.6 In addition to the description of the Lifecycle Management services and exclusions provided in the applicable Proposal, the following apply:

- a) Upon reasonable request by Motorola, Customer will provide a complete serial and model number list of the Equipment.
- b) Lifecycle Management 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 in this MSLMA or the applicable Proposal, Lifecycle Management 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 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 Lifecycle Management services.

3.2.7 The Lifecycle Management annualized price is based on the fulfillment of the two year cycle. If Customer terminates this service during a two year cycle, except for Motorola's default, then Customer will be required to pay for the balance of payments owed for the two year cycle if a major system release has been implemented before the point of termination.

3.2.8 If Customer terminates this Maintenance and Support or Lifecycle Management service and contractual commitment before the end of the **5** year term, for any reason other than Motorola's default, then the Customer will pay to Motorola a termination fee equal to the discount applied to the last three years of service payments related to the **5** year commitment. This provision survives the expiration or termination of the Agreement and applies notwithstanding any contrary provision.

Section 4. Payment

4.1 Unless alternative payment terms are stated in this MSLMA, Motorola will invoice Customer in advance for each payment period. All other charges will be billed monthly and the Customer must pay each invoice in U.S. dollars within thirty (30) days of the invoice date. Customer will reimburse Motorola for all property taxes, sales and use taxes, excise taxes, and other taxes or assessments that are levied as a result of Services rendered under this Agreement (except income, profit, and franchise taxes of Motorola) by any governmental entity.

4.2 INFLATION ADJUSTMENT. For multi-year agreements, at the end of the Agreement's first year and each year thereafter, a CPI percentage change calculation shall be performed using the U.S. Department of Labor, Consumer Price Index, "All Items," Unadjusted Urban Areas (CPI-U). Should the annual inflation rate increase greater than 3% during the previous year, Motorola shall have the right to increase all future maintenance prices by the CPI increase amount exceeding 3%. The adjustment calculation will be based upon the CPI for the most recent twelve (12) month increment beginning from the most current month available posted by the U.S. Department of Labor (<http://www.bls.gov>) immediately preceding the new maintenance year. For purposes of illustration, if in Year 5 the CPI reported an increase of 8%, Motorola may increase the Year 6 price by 5% (8%-3% base).

Exhibit A
PAYMENT

Except for a payment that is due on the Effective Date, Customer will make payments to Motorola within thirty (30) days after the date of each invoice. Customer will make payments when due in the form of a check, cashier's check, or wire transfer drawn on a U.S. financial institution. If Customer has purchased additional Professional or Subscription services, payment will be in accordance with the applicable addenda. Payment for the System purchase will be in accordance with the following milestones.

System Purchase (excluding Subscribers, if applicable)

- 1. 25% of the Contract Price due upon contract execution (due upon effective date);**
- 2. 40% of the Contract Price due upon shipment of equipment from Staging;**
- 3. 30% of the Contract Price due upon installation of equipment; and**
- 4. 5% of the Contract Price due upon Final Acceptance.**

If Subscribers are purchased, 100% of the Subscriber Contract Price will be invoiced upon shipment (as shipped).

Motorola shall make partial shipments of equipment and will request payment upon shipment of such equipment. In addition, Motorola shall invoice for installations completed on a site-by-site basis or when professional services are completed, when applicable. The value of the equipment shipped/services performed will be determined by the value shipped/services performed as a percentage of the total milestone value. Unless otherwise specified, contract discounts are based upon all items proposed and overall system package. For invoicing purposes only, discounts will be applied proportionately to the FNE and Subscriber equipment values to total contract price. Overdue invoices will bear simple interest at the maximum allowable rate by state law.

Motorola's proposal is conditioned upon the ability of Motorola to complete the project at the prices set forth herein. Due to significant market volatility and material price fluctuations in raw materials, Motorola reserves the right to review all material pricing prior to placing any order for materials or equipment required in order to verify price validity. In the event of a cost increase in material, equipment or energy occurring during performance of the project through no fault of Motorola, the contract price, time of completion and/or contract requirements shall be equitably adjusted by Change Order in accordance with the procedures of the contract documents. The freight rates are estimated. Motorola reserves the right to apply a fuel surcharge to the quoted freight rates on all shipments based on the cost of diesel at the time of shipment.

For Lifecycle Support Plan and Subscription Based Services:

Motorola will invoice Customer annually in advance of each year of the plan.