CITY OF
FREMONT
NEBRASKA

400 East Military Avenue, Fremont, NE 68025-5141

PSAP GOVERNANCE BOARD MEETING

Meeting Room – 1st Floor Police Dept
725 N. Park Ave, Fremont
December 2, 2025 7:30 a.m.

AGENDA

1. Meeting called to order

2. Open Meeting Act

3. Roll Call

4. Approve minutes of July 9, 2025, meeting.

5. Report and action for agreement with Fremont Public Schools for access to their camera system in emergencies.

6. Report and action on agreement with Motorola Solutions for radio system dispatch consoles for new communications center in new police building.

7. Information only - update on county radio system.

8. Adjourn

A current copy of the meeting agenda is available in the Communications Center at 725 N. Park

CITY OF
FREMONT
NEBRASKA PATHFINDERS

July 8, 2025
PSAP GOVERNANCE BOARD MEETING
MINUTES
Meeting Room – 1st Floor Police Dept.
725 N. Park Ave, Fremont
9:00 a.m.

A meeting of the Fremont/Dodge County PSAP Governing Board was held on July 8, 2025, in the first floor meeting room of the Fremont Police Department at 725 N. Park Avenue, Fremont, Nebraska. The meeting was called to order by Chairman Joey Spellerberg at 9:00 a.m. The meeting was preceded by a publicized notice in the Fremont Tribune and the agenda displayed in the Fremont Police/PSAP lobby and is open to the public. A copy of the open meeting law is available for public inspection.

Roll call showed Board Members Joey Spellerberg, Doug Backens, Blair Horner, Bob Missel and Mark Jensen present in the room. James Vaughan and Greg Beam were absent. 5 present, 2 absent. Communications Director Shelly Holzerland and Radio Administrator Tom Christensen, ex-offico present. Guests were City Administrator Jody Sanders and Lead Dispatcher Jamie Carlson via Teams.

The draft minutes of the April 29, 2025 meeting were distributed at the meeting. Mr. Jensen moved to accept the minutes of the April 29th meeting and Mr. Horner seconded the motion.

Vote: Aye: Spellerberg, Backens, Horner, Missel, Jensen
No: None Motion passed

Request and action for funding replacement parts for one 24/7 dispatch position desk.

The motors on one of the Xybix 24/7 ergonomic desks has quit working. The equipment is 12 years old, and the existing motors are not repairable. IT and Xybix spent several hours troubleshooting, trying to get them to work but were unsuccessful. The desk is stuck in one position and cannot be moved to accommodate different sized users.

There are sufficient funds in the capital budget lines for projects that are not going to be done this year. The current situation is not sustainable until the new building is complete. The purchase will be sole source as Xybix will be able to reuse a large portion of the existing desk, thus reducing the costs.

Mr. Missel moved to replace the desk with the quote from Xybix as presented. Mr. Jensen seconded the motion.

Vote: Aye: Spellerberg, Backens, Horner, Missel, Jensen
No: None   Motion passed

Report on damage and troubleshooting at the radio tower site at Dodge.

Tom Christensen, County Radio Administrator, reports that on June 16th, 2025, a severe thunderstorm caused a lightening strike at the Dodge tower site. The lightning actually hit the ground and traveled through to cause damage to the tower. The tower is still operational, having damage to the tower top amp and surge suppression system. The tower is covered by insurance through NIRMA, with a $2500 deductible. Once the deductible is reached, NIRMA will pay the remainder. Tom estimates it could be as high as $20,000.

The tower crew came out July 3rd and did some repair/troubleshooting. Once their invoice is paid, it will cover the deductible. A tower crew/climb was budgeted so there is sufficient money in the budget to pay this expense.

Report Only – No Action Taken

With no further business, Mr. Missel moved to adjourn at 9:15 a.m.   Mr. Backens seconded.

Vote: Aye: Spellerberg, Backens, Horner, Missel, Jensen
No: None   Motion passed

Respectfully
Shelly Holzerland
FDCC Communications Director

INTERLOCAL AGREEMENT

BETWEEN THE FREMONT PUBLIC SCHOOL DISTRICT AND THE FREMONT/DODGE COUNTY COMMUNICATIONS, FOR EMERGENCY SITUATION ACCESS TO DISTRICT GENETEC SECURITY CAMERAS,

This Interlocal Agreement ("Agreement") is entered into by and between the Fremont Public School District (District) and the Fremont/Dodge County Communications (FDCC), on the 27 of October, 2025. The District and FDCC may be individually referred to as a "Party" or collectively as "Parties."

RECITALS

WHEREAS, the District operates various school sites and has installed video surveillance cameras ("Security Cameras") to provide a safe educational environment for students and District employees; and

WHEREAS, the County of Dodge, Nebraska (herein referred to as "DODGE"), and the City of Fremont, Nebraska (herein referred to as "FREMONT"), own and operate a joint communications and dispatch center for 911 calls and it is referred to as the "Fremont/Dodge County Communications Center" ("FDCC")

WHEREAS, the Fremont Police Department, part of "FREMONT" is primarily responsible for providing safety and welfare of Fremont residents, including District students and employees at District school sites and their respective officers are dispatched to emergency situations through the FDCC; and

WHEREAS, the District and the FDCC recognize the need for a shared understanding as to the use of Security Cameras in the schools in a way that enhances security and aids law enforcement while respecting the privacy expectations of members of the school community.

WHEREAS, the parties wish to enter into such an Agreement pursuant to the terms of the Interlocal Cooperation Act (Nebraska Revised Statutes §13-801 through §13-827); and

THEREFORE, the Parties agree as follows:

1. **Purpose**. The purpose of this Agreement is to set forth guidelines for the District and FDCC as to the role and responsibilities of each in the use of Security Cameras and surveillance in District schools.

2. **FDCC Access to Security Cameras**: EMERGENCY SITUATION ACCESS. In the event of an emergency situation, as determined by the District, which includes active shooters, bomb threats, or any other immediate threat to life, limb, or safety of building occupants, the Emergency Button shall be activated by the affected building personnel triggering FDCC access to real-time footage at that building.
Access is strictly limited to the duration of the emergency and is restricted to the specific site of the incident. Access shall end once the emergency is contained or resolved. In the event of a false

activation, FDCC shall end the access as soon as they are made aware of a false activation.

3. **Dissemination**. FDCC shall not disseminate, in any way to any third party, real-time footage or video recordings from the Security Cameras. Law Enforcement requests for the release of recorded material must be made through an Administrative Subpoena, warrant, or Court Order directed to the Districts Superintendent's Office.

4. **Training**. All FDCC personnel with access to the Security Cameras or video recordings shall be instructed in the technical and ethical parameters of appropriate camera use and shall receive a copy of this policy and provide a written acknowledgment that they have read and understood its contents.

The District shall assist with providing training as requested by FDCC. FDCC shall provide an Annual Training Report (due on August 1st of each year of the Agreement), providing the following information related to each training session in which FDCC accesses the District's Security Cameras: Date/time of access, name of FDCC personnel who accessed the Security Cameras, site location and camera number. FDCC shall not download, record, or store any video footage obtained under this Agreement except as authorized by law enforcement subpoena or court order.
Training dates shall be scheduled when school is not in session, (weekends, holidays, school vacation days, etc.)

5. **Monitor of Use**. FDCC access to the Security Cameras shall remain off unless an "Emergency Situation" as defined in Paragraph 2 of this Agreement.

6. **Confidential List of Designated FDCC Personnel for Security Camera Access**. The FDCC shall provide the District a confidential spreadsheet of designated FDCC personnel who are authorized access to the Security Cameras during an Emergency Situation. Only those individuals listed on the list will have access to the Security Cameras during emergency situations.

The FDCC shall provide the name, position, rank and supervisors' contact information. This spreadsheet shall be updated as FDCC personnel are hired, retired, or resign from their positions.

7. **Access**. Authorized FDCC individuals shall be provided with access via the Genetec Federation. Access will be limited to the cameras located at the emergency site, as outlined in Paragraph 2 of this Agreement.

8. **Confidentiality**. FDCC acknowledges that in viewing Security Camera access and video footage as provided under this Agreement, FDCC may come into possession of information that may be considered confidential student information pursuant to the Family Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) and other applicable Nebraska State Law.

Should this information also become part of the Fremont Police Department's investigation, it will also become an investigative document and not be a public record pursuant to Neb. Rev. Stat. §84-712.05(5). It is the District's obligation to determine whether any information obtained through this Agreement constitutes confidential student information. FDCC will take all necessary steps to protect, and maintain the confidentiality of such information, ensuring it is only accessible to those personnel who need it to fulfill their job functions.

In the event of an accidental disclosure of Confidential Information, either to a third party or employee who does not require access, FDCC shall take all necessary steps to secure the return of such information and shall inform the District within twenty-four (24) hours of disclosure.

FDCC shall defend, indemnify and hold harmless the District, it's officers, employees and agents from any and all claims, damages, liabilities, or expenses that in anyway relate to the breach of this provision, including, without limitation, the disclosure of Confidential Information, whether knowingly or unknowingly, intentionally or unintentionally, or using footage obtained from the District's video surveillance cameras for a use other than the uses specified herein, except as required by law or a court order.

9. **No Waiver of Constitutional Rights**. The Parties agree that through this Agreement, the District is in no way waiving its, its employees, or its student's rights to be free from unreasonable searches and seizures pursuant to either federal or state law.

10. **Termination**. Either Party may terminate this Agreement at any time with written 10 days' notice to the other Party.

11. **Notice**. Any notice required or permitted to be given under this Agreement shall be deemed to have been given, served, and received if given in writing and either personally delivered or deposited in the United States mail, registered or certified mail, postage prepaid, return receipt required, or sent by overnight delivery service, addressed as follows:

FREMONT PUBLIC SCHOOL DISTRICT
Brad Dahl, Superintendent
130 East 9th Street Fremont, NE 68025
402-727-3002

PSAP GOVERNANCE BOARD
Shelly Holzerland,
Communications Director
725 North Park Avenue
Fremont, NE 68025
402-727-2677

12. **Authority of the Executing Officer or Party**. By signing below, the signer represents that it has the legal right, power, and authority to enter into and execute this Memorandum and to bind the Party on whose behalf the signer executes this Agreement.

13. **Effective Date:** The effective date of this Agreement shall be the date which all Parties have signed and approved this Agreement. The parties understand that the Agreement will need to be taken to each's governing bodies for final vote approval.

14. **Agreement Term:** The term of this Agreement shall be for three (3) years from the effective date of this Agreement, unless terminated as hereinafter provided. This Agreement may be extended for additional three (3) year periods by mutual written agreement of the parties.

15. **Modification:** This Agreement may not be modified, altered, changed, or amended except by written instrument executed by all Parties hereto.

16. **Severability:** If it shall be determined by a court or other governmental body of competent jurisdiction that any provision of this Agreement shall be invalid or unenforceable under any applicable law, such invalidity or unenforceability shall not invalidate the entire Agreement and shall not affect the other terms and provisions of this Agreement. To the extent legally possible, any invalid or unenforceable provision will be modified to reflect the parties' original intention.

17. **Singulars/Plurals/Context:** Whenever required by the context, the singular shall include the plural, the plural the singular, and one gender shall include all genders. When not inconsistent with the context, words used in the present tense include the future. The words "shall" and "will" are mandatory, and the word "may" is permissive.

18. **Caption Headings:** Caption Headings in this Agreement are for convenience only and are not to be used to interpret or define the provisions of the Agreement.

19. **Full Integration:** This is a fully integrated Agreement and supersedes any and all prior Agreements, whether oral or written, between the parties; and, this Agreement embodies a full and complete understanding of the parties.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement by their respective representatives, each thereunto duly authorized, on the Effective Date.

APPROVED AS TO FORM:

FREMONT PUBLIC SCHOOL
DISTRICT (DISTRICT)
By____________________
Name:
10-27-2025

PSAP GOVERNANCE BOARD

By:
____

APPROVED AS TO FORM:

Name:____
Title:____

Executed and Adopted this ____________ day of ________________, 2025, by the City of Fremont, Nebraska:

Executed and Adopted this ____________ day of _________________, 2025, by the City of Fremont, Nebraska:

ATTEST: THE CITY OF FREMONT, NEBRASKA:

______________________________ ________________________________

City Clerk Mayor

Executed and Adopted this _____________ day of __________________, 2024, by the County of Dodge, Nebraska:

ATTEST: THE COUNTY OF DODGE, NEBRASKA:

__________________________ _____________________________________

County Clerk Chairman

MOTOROLA SOLUTIONS

Proposal

NE, City of Fremont

Command Central AXS Dispatch Console

Firm Proposal

October 20, 2025

Motorola Solutions, Inc.
500 West Monroe St, Ste 4400
Chicago, IL 60661

10/20/2025

Shelly Holzerland
Fremont Police Department
725 North Park Avenue
Fremont, NE 68025

RE: City of Fremont Police Department AXS Dispatch Consoles

Dear Shelly,

Motorola Solutions, Inc. (“Motorola Solutions”) appreciates the opportunity to present the Fremont Police Department with this proposal to provide updated dispatch consoles for the City of Fremont/ Dodge County 911 Center.

This proposal consists of:

- 6 AXS Dispatch Positions
  - All 6 positions will be located in the new Fremont Police Department and will be core connected to the ORION system.
- 8 Consolettes
- Onsite Training
  - Onsite Training will be provided for 2 administrators and 11 dispatchers.

This proposal includes the necessary equipment, licenses, as well as a System Technologist to implement the project. This proposal remains valid until December 12, 2025 and subject to the terms of Contract No. 111563 O4 between Motorola Solutions, Inc. and the State of Nebraska. The City of Fremont, may accept this proposal by issuing a Purchase Order or a signed Notice To Proceed document.

Any questions regarding this proposal can be directed Nicole Kingston, Senior Account Manager at 402-919-8754 or emailed to Nicole.Kingston@motorolasolutions.com

We thank you for the opportunity to present our proposed solution, and we hope to strengthen our relationship by implementing this project.

Sincerely,

Fran Cueva
Area Sales Manager - Iowa & Nebraska
Motorola Solutions, Inc

Table of Contents

Section 1

Section 2

Section 3

Section 7

Section 8

Section 9

Section 1

System Description

1.1 Overview

Motorola Solutions, Inc.'s (Motorola) CommandCentral AXS Dispatch Console reduces the barriers between systems in City of Fremont'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.

This 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.

1.1.1 Integration with the ASTRO® 25 Network

The proposed dispatch console seamlessly integrates into the Omaha Regional Interoperability Network (ORION) ASTRO® 25 system for an integrated, mission-critical network. This tight union between radio infrastructure and console equipment has several operational benefits to the City of Fremont. 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 to ASTRO® 25 System

The ASTRO® 25 system's architecture is flexible and can be configured to meet the City of Fremont's unique needs.

Dual Site Link

The proposed console site for City of Fremont 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 and City of Fremont'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.

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.

Advanced Conventional

This option provides the dispatcher with the ability to control ASTRO® 25 conventional channels and/or MDC 1200 channels.

1.1.3 Conventional Base Station Interfaces

The proposed consoles access and control City of Fremont's analog and digital conventional base stations through the use of Conventional Channel Gateways (CCGW). The console processes audio received from the station and controls various features on the stations, such as frequency selection, private line selection, and repeater on/off.

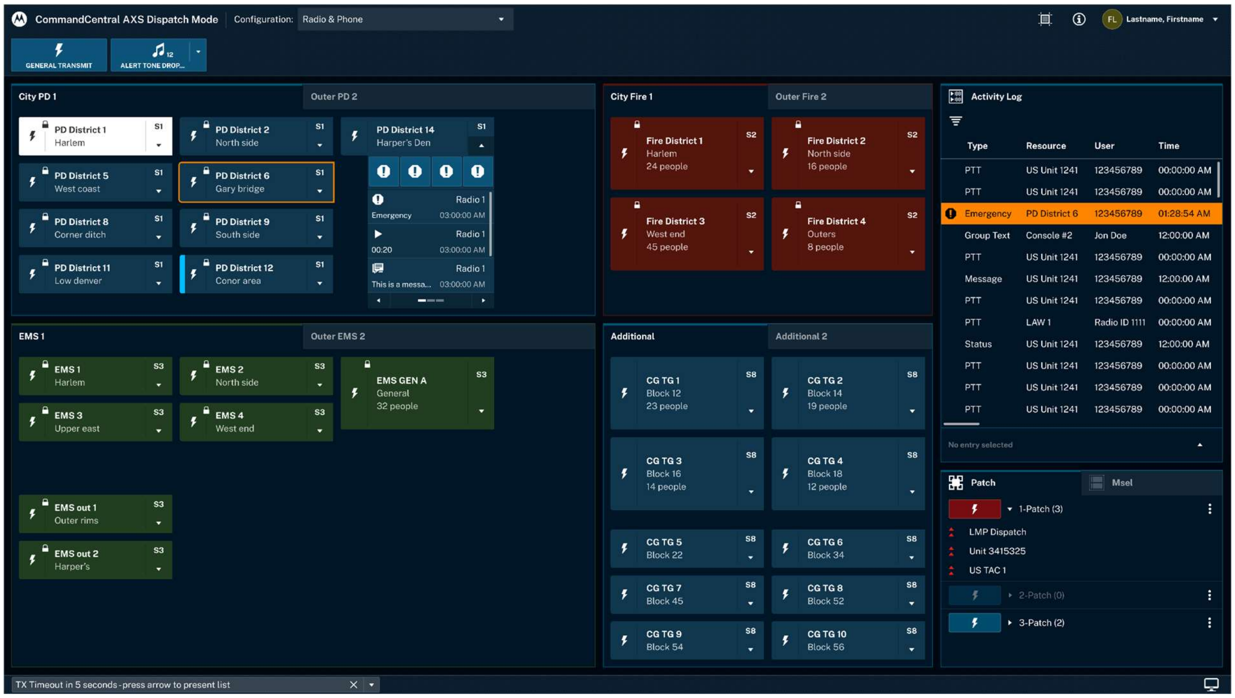
Additionally, the CCGWs allow for recovery of MDC 1200 and digital signaling, such as unit ID and emergency alarm.

1.2 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.

1.2.1 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.


CommandCentral AXS Dispatch Mode
Lastname, Firstname
GENERAL TRANSMIT
ALERT TONE DROP...
City PD 1
Outer PD 2
PD District 1 Harlem S1
PD District 2 North side S1
PD District 14 Harper's Den S1
PD District 5 West coast S1
PD District 6 Gary bridge S1
PD District 8 Corner ditch S1
PD District 9 South side S1
PD District 11 Low denver S1
PD District 12 Conor area S1
Radio 1
Emergency 03:00:00 AM
00:20 03:00:00 AM
This is a messa... 03:00:00 AM
City Fire 1
Outer Fire 2
Fire District 1 Harlem 24 people S2
Fire District 2 North side 16 people S2
Fire District 3 West end 45 people S2
Fire District 4 Outers 8 people S2
EMS 1
Outer EMS 2
EMS 1 Harlem S3
EMS 2 North side S3
EMS GEN A General 32 people S3
EMS 3 Upper east S3
EMS 4 West end S3
EMS out 1 Outer rims S3
EMS out 2 Harper's S3
Additional
Additional 2
CG TG 1 Block 12 23 people S8
CG TG 2 Block 14 19 people S8
CG TG 3 Block 16 14 people S8
CG TG 4 Block 18 12 people S8
CG TG 5 Block 22 S8
CG TG 6 Block 34 S8
CG TG 7 Block 45 S8
CG TG 8 Block 52 S8
CG TG 9 Block 54 S8
CG TG 10 Block 56 S8
Activity Log
No entry selected
Patch
Msel
1-Patch (3)
LMP Dispatch
Unit 3415325
US TAC 1
2-Patch (0)
3-Patch (2)

Configuration: Radio & Phone

Type	Resource	User	Time
PTT	US Unit 1241	123456789	00:00:00 AM
PTT	US Unit 1241	123456789	00:00:00 AM
Emergency	PD District 6	123456789	01:28:54 AM
Group Text	Console #2	Jon Doe	12:00:00 AM
PTT	US Unit 1241	123456789	00:00:00 AM
Message	US Unit 1241	123456789	12:00:00 AM
PTT	US Unit 1241	123456789	00:00:00 AM
PTT	LAW 1	Radio ID 1111	00:00:00 AM
Status	US Unit 1241	123456789	12:00:00 AM
PTT	US Unit 1241	123456789	00:00:00 AM
PTT	US Unit 1241	123456789	00:00:00 AM
PTT	US Unit 1241	123456789	00:00:00 AM

TX Timeout in 5 seconds - press arrow to present list

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.

1.2.2 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.

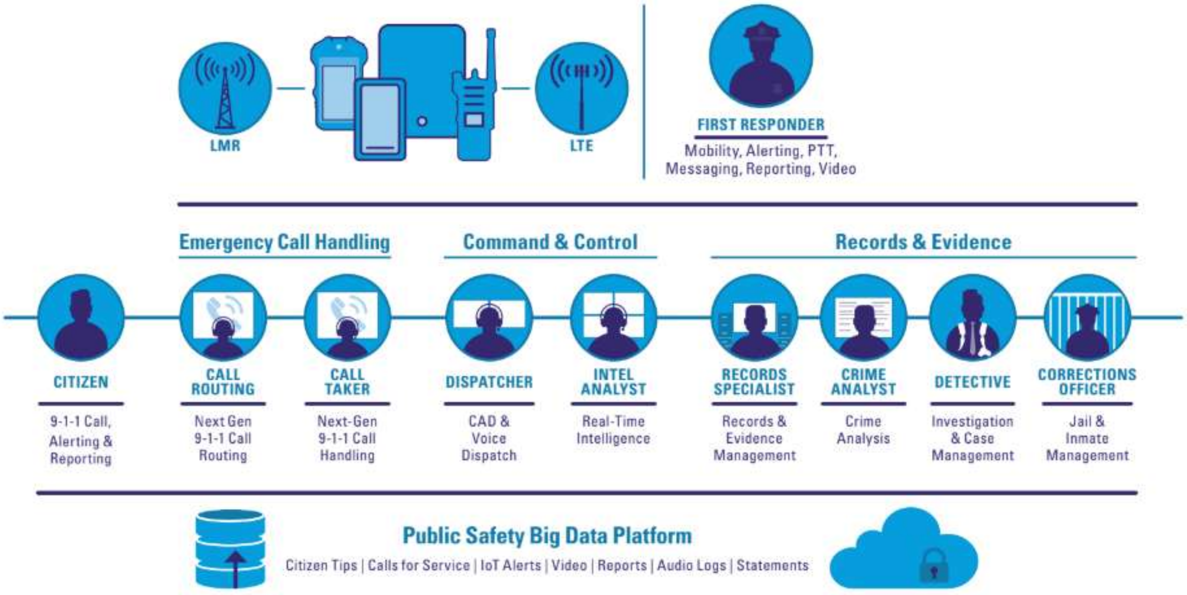

LMR
LTE
FIRST RESPONDER
Mobility, Alerting, PTT, Messaging, Reporting, Video
Emergency Call Handling
Command & Control
Records & Evidence
CITIZEN
9-1-1 Call, Alerting & Reporting
CALL ROUTING
Next Gen 9-1-1 Call Routing
CALL TAKER
Next-Gen 9-1-1 Call Handling
DISPATCHER
CAD & Voice Dispatch
INTEL ANALYST
Real-Time Intelligence
RECORDS SPECIALIST
Records & Evidence Management
CRIME ANALYST
Crime Analysis
DETECTIVE
Investigation & Case Management
CORRECTIONS OFFICER
Jail & Inmate Management
Public Safety Big Data Platform
Citizen Tips | Calls for Service | IoT Alerts | Video | Reports | Audio Logs | Statements

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 City of Fremont's 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.

1.2.3 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.

1.2.4 Auxiliary Inputs/Outputs

The proposed console supports Global Auxiliary Inputs/Outputs (Aux I/Os) for remote status indications or remote control through dispatch positions. Global Aux I/Os are typically implemented by hardware that is independent of the dispatch positions in a system and may be accessible to multiple dispatch positions. Aux I/O Servers provide the Aux I/O feature for the consoles.

1.2.5 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.

1.2.6 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 City of Fremont's 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.

1.2.7 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).

1.2.8 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.

1.2.9 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 Protecting Consoles and Communications

The console enables end-to-end encryption from the dispatcher to the ASTRO® 25 network, so that City of Fremont's 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.

1.3.1 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.

1.3.2 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 (AES, DES-OFB, and/or ADP) and multiple secure keys.

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.

1.3.3 Securing Communications at the Logging Recorder

Not only are real-time communications encrypted, encryption extends to call logging to ensure that even recorded communications are not vulnerable to retrieval by unauthorized people. The AIS can support different encryption algorithms simultaneously.

Like the dispatch console, the AIS also requires a valid radio system user account name and password be entered and validated by the radio system's network manager before it allows access to recorded information. A user can access only the recordings for which the user has access rights. This enables agencies to keep their logs private from other agencies on the same system.

1.3.4 Key Management via Key Variable Loader (KVL)

Key management via a key variable loader (KVL) feature provides the ability to manage all the keys for an AXS Console or archiving interface server using only a KVL.

1.4 Incorporating Console Configuration and Management

The proposed console system is configured and managed by the same configuration manager, fault manager, and performance reporting applications as the radio system. The user can define exactly which resources are available and how they are presented to the dispatcher. This provides City of Fremont with a single point for configuring and managing the entire ASTRO® 25 system. Changes are automatically distributed throughout the system.

This centralized approach saves valuable time and effort for system administrators and technicians and reduces the errors that can occur when radio IDs and other data are entered at multiple locations. In addition, call traffic and performance reports for each dispatch position can be generated from the system's network manager, enabling administrators to quickly and easily ensure optimal effectiveness and efficiency.

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, including a USB microphone, USB headset, and USB footswitch. The following list describes the components included in the proposed configuration.

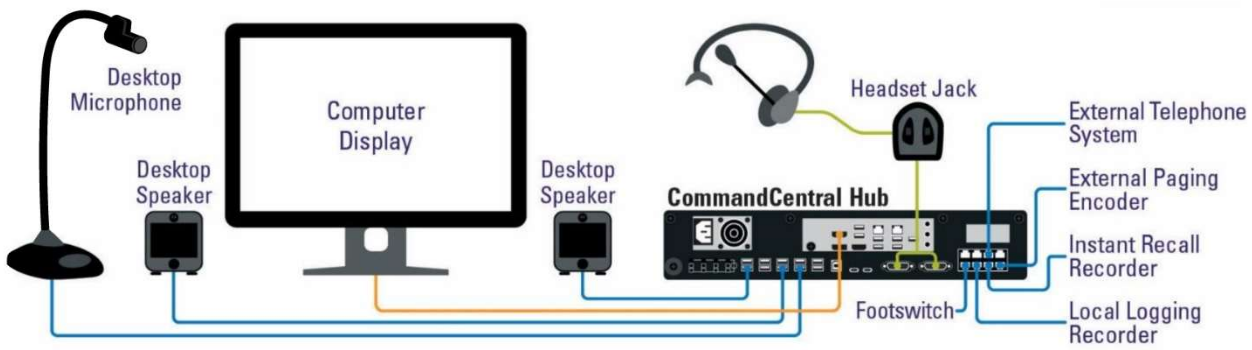


Figure 1-3: CommandCentral AXS Dispatch Console Accessories Example

Computer Display

The dispatch position will use a 24” Computer Display with non-touch.

B1956 CommandCentral Hub (CC Hub)

The CommandCentral Hub (CC Hub) is the platform on which the CommandCentral AXS Dispatch Console operates. The CC Hub contains a number of analog inputs and outputs for connecting various peripheral devices as well as a workstation class computer motherboard.

The PC that is internal to the CC Hub will be programmed with a Microsoft Windows based operating system (OS) image developed for the dispatch application.

Desktop Speakers

Four 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.

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.

Gooseneck 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.

Footswitch

Each dispatch position includes a dual pedal footswitch that controls general transmit and monitor functions.

Telephone/Headset Interface Port

The telephone/headset port provides a connection for an external telephone to the dispatch position. This allows the operator to use a single headset to communicate on both the radio system and an external telephone system.

External Paging Encoder Port

The external paging encoder port provides a connection for an optional external tone paging encoder to provide tone paging services via the dispatch console. Analog paging tones generated by the encoder are transmitted by the dispatch console on the selected trunked and/or conventional radio resource(s).

Local Logging Recorder Port

As an alternative or supplemental approach to an audio logging subsystem, the analog output port on the CommandCentral Hub allows an optionally available external logging recorder to be connected to a dispatch console. Long-term audio recording is used to record a portion of the inbound and outbound audio present on a specific dispatch position. These recordings are typically archived for long-term storage, and provide a historical record of the radio communications made at a given dispatch position.

The analog output port can be configured to log any combination of these audio sources, such as:

- Audio received from a currently selected radio.
- Microphone audio being transmitted by this dispatcher to the currently selected or unselected radio resources.
- Any tones generated by the dispatch position that appear in its speakers (trunking tones, emergency tones, etc.) or tones generated by an external paging encoder.

Private Aux I/O Port

The dispatch console supports four Private Aux I/O relays located on the CommandCentral Hub of the dispatch position. Each relay can be configured to support any one of the five functions or it can be configured to be unused.

- Call on Selected Channel
- Op PTT
- Emergency Beacon
- Activate Private Relay when Public Aux I/O is Active
- Select Phone Off Hook Relay

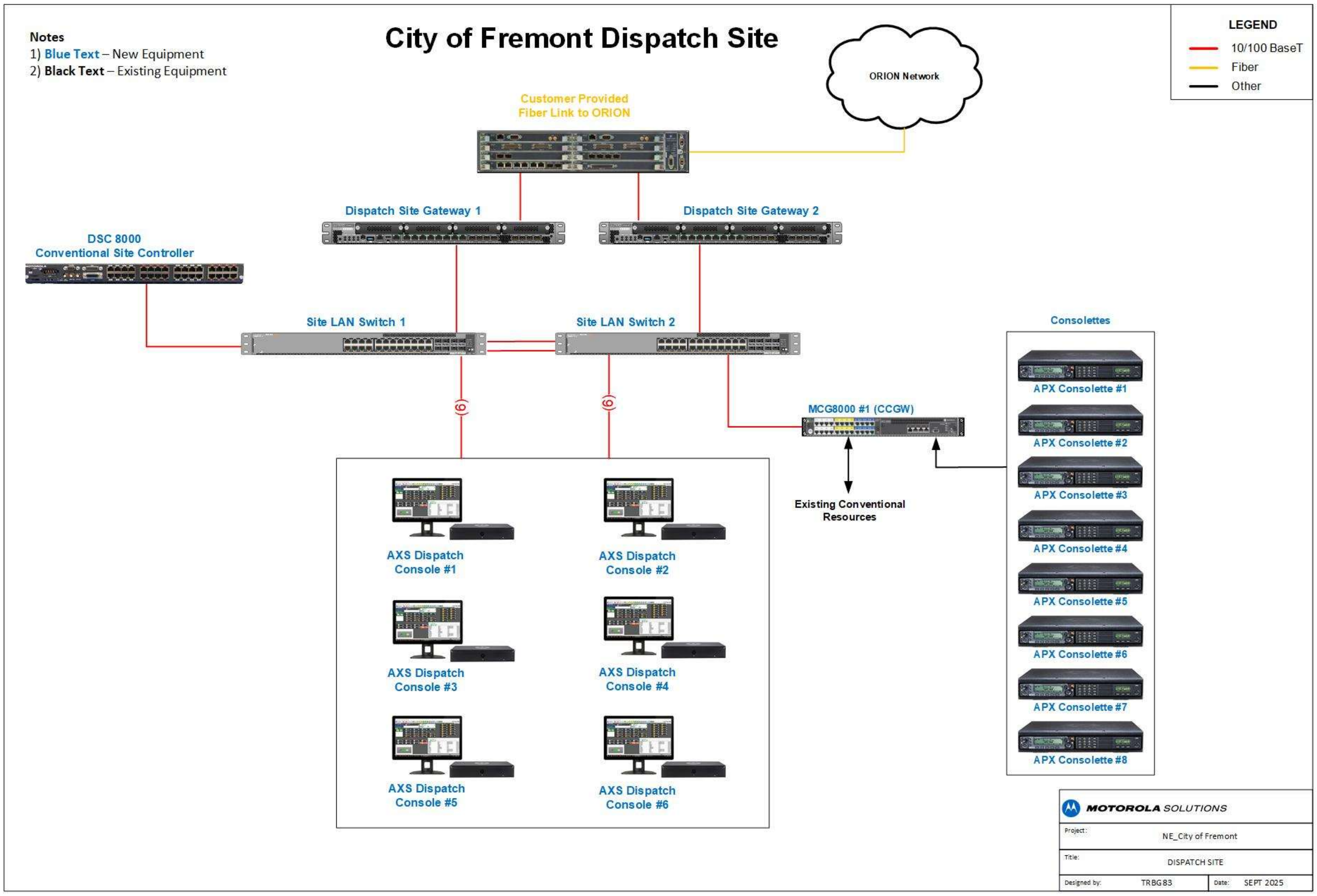
Redundant Ethernet Connection

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.

Section 2

System Diagrams

2.1 CommandCentral AXS Console Dispatch Site



Section 3

Equipment List

3.1 Dispatch CC AXS Console System Equipment Lists

3.1.1 ORION Core Licenses

QTY	NOMENCLATURE	DESCRIPTION
1	SQM01SUM0323A	ASTRO MASTER SITE
1	CA03517AD	ADD: CORE EXPANSION
2	UA00156AA	ADD: 5 CONSOLE OPS: AXS, MCC7500/E AND AIS

3.1.2 Network

QTY	NOMENCLATURE	DESCRIPTION
2	T8492A	SITE ROUTER & FIREWALL- AC
2	CA03445AA	ADD: MISSION CRITICAL HARDENING
2	CA03448AA	ADD: STATEFUL FIREWALL
2	CLN9066A	SWITCH,SWITCH,EX4100 24-PORT
2	CLN9105A	CABLE FRU, 1 METER JUNIPER DAC CABLE

3.1.3 OP Positions

QTY	NOMENCLATURE	DESCRIPTION
6	HKVN4729A	AXS DISPATCH CONSOLE LICENSE
6	HKVN4730A	AXS TRUNKING SERVICES LICENSE
6	HKVN4731A	AXS ADVANCED CONVENTIONAL SERVICES LICENSE
6	HKVN4732A	AXS SECURE VOICE SERVICES LICENSE
6	HKVN4733A	LICENSE,AXS INTEGRATED IRR
6	HKVN4736A	AXS AMBE+2 VOCODER ROYALTY AND LICENSE
6	HKVN4737A	AXS STANDARD LEVEL RADIO RESOURCE CAPACITY LICENSE
1	B1957A	AXS SOFTWARE DVD
6	B1956A	COMMANDCENTRAL HUB, W/CLIENT PC
6	CA03850AA	ADD: WINDOWS OS FOR MCC7500E CONSOLE

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions

QTY	NOMENCLATURE	DESCRIPTION
6	CA03553AA	ADD: AC LINE CORD, NORTH AMERICA
6	CA03547AA	ADD: BRACKET, MOUNTING 2RU
6	CA03583AA	ADD: FOUR CABLES, POWER 24VDC
6	CA03572AA	ADD: CABLE RETENTION BRACKET
12	B1913A	MCC SERIES HEADSET JACK
6	B1951B	DISPATCH DESKTOP MICROPHONE, USB
6	CA03413AA	ADD: USB CABLE, TYPE A TO TYPE C, 4.5M
24	B1952B	SPEAKER, DESKTOP, USB
24	CA03413AA	ADD: USB CABLE, TYPE A TO TYPE C, 4.5M
6	L3226A	COMPUTER MOUSE, CERTIFIED OPTICAL WHEEL MOUSE FOR RSD SERVERS AND WORKSTATIONS
6	L3225A	CERTIFIED KEYBOARD FOR RSD SERVERS AND WORKSTATIONS
6	RLN6098A	HDST MODULE BASE W/PTT, 15 FT CBL
6	DSTG241B	TECH GLOBAL EVOLUTION SERIES 24INCH NON TOUCH
6	DSTWIN6328A	PROVIDES ONE DUAL PEDAL FOOTSWITCH
6	T8742A	MCAFEE FOR WINDOWS CLIENT, A2019.2 +PLUS
6	T8806A	WINDOWS SUPP. TRANSPARENT, A2022.1

3.1.4 Nokia MPLS

QTY	NOMENCLATURE	DESCRIPTION
1	DSMW3HE06791AA	SAR-8 SHELF V2
1	DSMW3HE02784TA	SAR RELEASE 23.X BASIC OS LICENSE
1	DSMW3HE06792EA	FAN MODULE (SAR-8 SHELF V2) EXT TEMP -48VDC
2	DSMW3HE02774AB	CONTROL SWITCH MODULE V2 (CSMV2) 48V
2	DSMW3HE11473BK	PMC CARD W/ 4 GIG-E SFP BUNDLE (1) 3HE02782AA PMC, (4) 3HE00062CB SFP
2	DSMW3HE05838AA	250W 120/240V AC POWER CONVERTER
2	DSMW3HE05837BA	7705 AC POWER CONVERTER PIGTAIL - O-RING
1	DS90111918	19" CANTILEVER FLUSH MOUNT SHELF, 18" DEPTH, BLACK
2	DSMW3HE00027CA	SFP - GIGE SX - LC ROHS 6/6 DDM -40/85C
1	DSMW3HE00062CB	SFP – GIGE BASE-T RJ45 R6/6 DDM -40/85C

3.1.5 Equipment Rack

QTY	NOMENCLATURE	DESCRIPTION
2	TRN7343A	RACK 7.5'
2	DS1101990	SPD, SHIELDED RJ-45 JACK, SINGLE LINE GBE (1000MBPS) R56 COMPLIANT
4	DSTSJADP	RACK MOUNT GROUND BAR, 19 IN FOR TSJ AND WPH SERIES DATA SPDS
10	0784469Y02	BRACKET,BRKT, CBL SUPPORT
6	1483693Y01	INSULATOR, RACK GROUND BAR
2	2983724Y01	LUG, 2-HOLE RACK GND BAR
24	0310907C93	SCREW,MACHINED THREAD-METRIC-M6X1,STEEL,SCRMCH M6X1X16 STRPAN ZNCPHOS
2	3182602Y06	GROUNDING BUS BAR
3	DSACPS6N120SN8TT	AC POWER STRIP, 6 OUTLETS, SASD PROTECTED, UL1449/R56, 8FT CORD
3	DSACPS19RM	19IN RACK MOUNT BRACKET FOR ACPS POWER STRIP UNITS

3.1.6 Conventional Site Controller

QTY	NOMENCLATURE	DESCRIPTION
1	T8810A	STANDALONE DSC 8000 CONTROLLER
1	CA04079AA	ADD: ASTRO NEXT SYSTEM RELEASE 2024.X
1	CA03801AA	ADD: DSC 8000 CONVENTIONAL SITE CONTROLLER
1	UA00787AA	ADD: DSC 8000 CONVENTIONAL SITE CONTROLLER SW
1	CA03832AA	ADD: NM--DISPATCH SITE
1	T8811A	DSC AC POWER SUPPLY CHASSIS
1	CA03800AA	ADD: SINGLE POWER SUPPLY FOR DSC
1	CA03533AA	ADD: DSC AC POWER CABLE - US, 12 FT

3.1.7 CCGW

QTY	NOMENCLATURE	DESCRIPTION
1	SQM01SUM0333A	MCG 8000 CONVENTIONAL GATEWAY
1	CA03714AA	ADD: AC POWER
8	CA03717AA	ADD: ACIM INTERFACE
8	CA03719AA	ADD: DIGITAL IP INTERFACE
8	CA03720AA	ADD: ANALOG IP INTERFACE

3.1.8 Spares

QTY	NOMENCLATURE	DESCRIPTION
1	B1956A	COMMANDCENTRAL HUB, W/CLIENT PC
1	CA03850AA	ADD: WINDOWS OS FOR MCC7500E CONSOLE
1	CA03553AA	ADD: AC LINE CORD, NORTH AMERICA
1	CA03547AA	ADD: BRACKET, MOUNTING 2RU
1	CA03548AA	ADD: TWO CABLES, POWER 24VDC
1	CA03572AA	ADD: CABLE RETENTION BRACKET
1	B1913A	MCC SERIES HEADSET JACK
1	B1951B	DISPATCH DESKTOP MICROPHONE, USB
1	CA03413AA	ADD: USB CABLE, TYPE A TO TYPE C, 4.5M
1	B1952B	SPEAKER, DESKTOP, USB
1	CA03413AA	ADD: USB CABLE, TYPE A TO TYPE C, 4.5M
1	DSMW3HE06791AA	SAR-8 SHELF V2
1	DSMW3HE06792EA	FAN MODULE (SAR-8 SHELF V2) EXT TEMP -48VDC
1	DSMW3HE02774AB	CONTROL SWITCH MODULE V2 (CSMV2) 48V
1	DSMW3HE11473BK	PMC CARD W/4 GIG-E SFP BUNDLE (1) 3HE02782AA PMC, (4) 3HE00062CB SFP
1	DSMW3HE05838AA	250W 120/240V AC POWER CONVERTER
1	DSMW3HE05837BA	7705 AC POWER CONVERTER PIGTAIL – O-RING

3.1.9 Consolettes

QTY	NOMENCLATURE	DESCRIPTION
8	L37TSS9PW1CN	ALL BAND CONSOLETTE CN

QTY	NOMENCLATURE	DESCRIPTION
8	G90AC	ADD: NO MICROPHONE NEEDED APX
8	G851AG	ADD: AES/DES-XL/DES-OFB ENCRYP APX AND ADP
8	HA00694AA	ADD: 7Y ESSENTIAL SERVICE HTM
8	GA00580AA	ADD: TDMA OPERATION
8	CA01598AB	ADD: AC LINE CORD US
8	G51AT	SOFTWARE LICENSE SMARTZONE
8	L999AG	ADD: FULL FP W/E5/KEYPAD/CLOCK/VU
8	G806BL	SOFTWARE LICENSE ENH: ASTRO DIGITAL CAI OP APX
8	QA06898AA	ADD: SEQUENTIAL SERIAL NUMBER
8	QA09113AB	ADD: BASELINE RELEASE SW
8	W969BG	SOFTWARE LICENSE ENH: MULTIKEY OPERATION
8	G361AH	SOFTWARE LICENSE ENH: P25 TRUNKING SOFTWARE APX
8	HKN6233C	APX CONSOLETTE RACK MOUNT KIT
8	H1926B	MULTIPLEXER QMA APX CONSOLETTE

Section 4

Implementation Statement of Work

4.1 Responsibility Matrix

Motorola Solutions will install and configure the proposed equipment. The following table describes the tasks involved with installation and configuration.

Tasks	Motorola Solutions	Customer
PROJECT INITIATION		
Contract Finalization and Team Creation		
Execute contract and distribute contract documents.	X	X
Assign a Project Manager as a single point of contact.	X	X
Assign resources.	X	X
Schedule project kickoff meeting.	X	X
Deliverable: Signed contract, defined project team, and scheduled project kickoff meeting.		
Project Administration		
Ensure that project team members attend all meetings relevant to their role on the project.	X	X
Set up the project in the Motorola Solutions information system.	X	
Record and distribute project status meeting minutes.	X	
Maintain responsibility for third-party services contracted by Motorola Solutions.	X	
Complete assigned project tasks according to the project schedule.	X	X
Submit project milestone completion documents.	X	
Upon completion of tasks, approve project milestone completion documents.		X
Conduct all project work Monday thru Friday, 8 a.m. to 5:00 p.m. local time with the exception of Motorola Solutions' and the Customer's holidays.	X	
Deliverable: Completed and approved project milestones throughout the project.		

Tasks	Motorola Solutions	Customer
Project Kickoff		
Introduce team, review roles, and decision authority.	X	X
Present project scope and objectives.	X	
Review SOW responsibilities and project schedule.	X	X
Schedule Design Review.	X	X
Deliverable: Completed project kickoff and scheduled Design Review.		
Design Review		
Review the Customer's operational requirements.	X	X
Present the system design and operational requirements for the solution.	X	
Present installation plan.	X	
Present preliminary cutover plan and methods to document final cutover process.	X	
Present configuration and details of sites required by system design.	X	
Validate that Customer sites can accommodate proposed equipment.		X
Review safety, security, and site access procedures.	X	
Present equipment layout plans and system design drawings.	X	
Provide backhaul performance specifications and demarcation points.	X	
Provide heat load and power requirements for new equipment.	X	
Provide frequency and radio information for each site.		X
Assume liability and responsibility for providing all information necessary for complete installation.		X
Assume responsibility for issues outside of Motorola Solutions' control.		X
Ensure that frequency availability and licensing meet project requirements, and pay licensing and frequency coordination fees.		X
Review and update design documents, including System Description, Statement of Work, Project Schedule, and Acceptance Test Plan, based on Design Review agreements.	X	
Provide minimum acceptable performance specifications for customer provided hardware, software, LAN, WAN and internet connectivity.	X	

Tasks	Motorola Solutions	Customer
Execute Change Order in accordance with all material changes to the Contract resulting from the Design Review.	X	
Deliverable: Finalized design documentation based upon “frozen” design, along with any relevant Change Order documentation.		
SITE PREPARATION AND DEVELOPMENT		
Site Access		
Provide site owners/managers with written notice to provide entry to sites identified in the project design documentation.		X
Obtain site licensing and permitting, including site lease/ownership, zoning, permits, regulatory approvals, easements, power, and telco connections.		X
Deliverable: Access, permitting, and licensing necessary to install system equipment at each site.		
Site Planning		
Provide necessary buildings for installation of system equipment.		X
Provide the R56 requirements for space, power, grounding, HVAC, and connectivity requirements at each site.	X	
Provide adequate electrical power in proper phase and voltage at sites.		X
Provide backup power, as required.		X
Confirm that there is adequate utility service to support the new equipment and ancillary equipment.		X
Provide power to the top of each proposed rack.		X
Provide appropriately sized breakers in the AC panel at sites to support the needs of the proposed system.		X
Conduct site walks to collect pertinent information (e.g. location of telco, power, structures, etc.)	X	
Ensure that each site meets the R56 standards for space, grounding, power, HVAC, and connectivity requirements.		X
Prepare and submit Electromagnetic Energy (EME) plans for the site (as licensee) to demonstrate compliance with FCC RF Exposure Guidelines.		X
Obtain the permits needed to complete site development, including electrical, building, and construction permits.	X	
Pay for application fees, taxes, and recurring payments for lease/ownership of property.		X
Deliverable: Information and permitting requirements completed at each site.		

Tasks	Motorola Solutions	Customer
General Facility Improvements		
Provide adequate HVAC, grounding, lighting, cable routing, and surge protection based upon Motorola Solutions' Standards and Guidelines for Communication Sites (R56)		X
Ensure the resolution of environmental and hazardous material issues at each site including, but not limited to, asbestos, structural integrity (tower, rooftop, water tank, etc.), and other building risks.		X
Ensure that electrical service will accommodate installation of system equipment, including isolation transformers, circuit breakers, surge protectors, and cabling.		X
Provide obstruction-free area for the cable run between the demarcation point and system equipment.		X
Provide structure penetrations (wall or roof) for transmission equipment (e.g. antennas, microwave radios, etc.).		X
Supply interior building cable trays, raceways, conduits, and wire supports.		X
Pay for usage costs of power and generator fueling, both during the construction and installation effort, and on an ongoing basis.		X
Correct any R56 deficiencies.		X
Transport removed site equipment to a location designated by Customer and within Customer's jurisdiction.		X
Deliverable: Sites meet physical requirements for equipment installation.		
SYSTEM INSTALLATION		
Equipment Order and Manufacturing		
Create equipment order and reconcile to contract.	X	
Manufacture Motorola Solutions-provided equipment necessary for the system based on equipment order.	X	
Procure non-Motorola Solutions equipment necessary for the system.	X	
Deliverable: Equipment procured and ready for shipment.		
Equipment Shipment and Storage		
Provide a secure location for solution equipment.		X
Pack and ship solution equipment to the identified, or site locations.	X	
Receive solution equipment.		X
Inventory solution equipment.	X	

Tasks	Motorola Solutions	Customer
Deliverable: Solution equipment received and ready for installation		
General Installation		
Deliver solution equipment to installation location.	X	
Coordinate receipt of and inventory solution equipment with designated contact.	X	
Install all proposed fixed equipment as outlined in the System Description based upon the agreed-upon floor plans, connecting audio, control, and radio transmission cables to connect equipment to the power panels or receptacles, and audio/control line connection points. Installation performed in accordance with R56 standards and state/local codes.	X	
Provide system interconnections that are not specifically outlined in the system design, including dedicated phone circuits, microwave links, or other types of connectivity.		X
Install and terminate all network cables between site routers and network demarcation points, including microwave, leased lines, and Ethernet.	X	
Ensure that Type 1 and Type 2 AC suppression is installed to protect installed equipment.		X
Connect installed equipment to the provided ground system within 15 feet.	X	
Label Motorola-supplied equipment, racks, and cables.	X	
Perform preliminary audit of installed equipment to ensure compliance with requirements and R56 standards.	X	
Note any required changes to the installation for inclusion in the “as-built” system documentation.	X	
Remove, transport, and dispose of old equipment.		X
Deliverable: Equipment installed.		
Site Link Assessment		
Verify site link performance, prior to the interconnection of the solution equipment to the link equipment. Site links will be tested once. If the links do not pass the audit, a change order will be processed to perform link audits a second time after the customer resolves the link issues and prior to cutover.	X	
Motorola Solutions will not perform any work on non-Motorola Solutions owned equipment.		X
Provide information on customer public Internet connection for evaluation purposes.		X
Evaluate customer’s network from an IT perspective.	X	
Deliverable: Site Link Assessment completed and findings are presented to the Customer.		

Tasks	Motorola Solutions	Customer
Console Installation and Configuration		
Provide console furniture and make room for new console installation.		X
Identify circuits for connection to console and a demarcation point located within 25 feet of the console interface.		X
Connect console to circuit demarcation points.	X	
Install CommandCentral Hub and all associated console equipment at each position.	X	
Install peripheral console equipment in accordance with R56 standards and state/local codes.	X	
Develop templates for console programming.	X	
Perform console programming and configuration.	X	
Deliverable: Console equipment installation completed.		
Control Station Installation and Configuration		
Provide the locations of control stations at each site.		X
Survey mounting locations and develop control station installation plan.	X	
Provide adequate space, grounding, and power for the control station installation.		X
Properly ground the cabling, which will be run to the outdoor antenna location using the least obtrusive method.		X
Provide an elevated antenna mounting location, and adequate feed-line routing and support.		X
Install line (not greater than 100 feet in length) and antenna system (connectors, coax grounding kit, antenna, and surge protection).		X
Install RF local control stations identified in the equipment list.	X	
Provide existing control station codeplugs or provide a list of channels (and associated parameters) to program the proposed control stations.		X
Perform control station programming.	X	
Deliverable: Control station equipment installation completed.		
SYSTEM OPTIMIZATION AND TESTING		
R56 Site Audit		
Perform R56 site-installation quality-audits, verifying proper physical installation and operational configurations.	X	

Tasks	Motorola Solutions	Customer
Create site evaluation report to verify site meets or exceeds requirements, as defined in Motorola Solutions’ R56 Standards and Guidelines for Communication Sites.	X	
Deliverable: R56 Standards and Guidelines for Communication Sites audits completed successfully.		
Solution Optimization		
Verify that all equipment is operating properly and that all electrical and signal levels are set accurately.	X	
Verify that all audio and data levels are at factory settings.	X	
Verify communication interfaces between devices for proper operation.	X	
Ensure that functionality meets manufacturers' specifications and complies with the final configuration established during design review or system staging.	X	
Reconfigure and reoptimize 3rd party equipment that is not part of the Motorola Solutions scope of work.		X
Deliverable: Completion of System Optimization.		
Functional Acceptance Testing		
Verify the operational functionality and features of the solution supplied by Motorola Solutions, as contracted.	X	
Witness the functional testing.		X
Document all issues that arise during the acceptance tests.	X	
If any major task for the system as contractually described fails during the Customer acceptance testing or beneficial use, repeat that particular task after Motorola Solutions determines that corrective action has been taken.	X	
Resolve any minor task failures before Final System Acceptance.	X	
Document the results of the acceptance tests and present for review.	X	
Review and approve final acceptance test results.		X
If any major task as contractually described fails, repeat that particular task after Motorola Solutions determines that corrective action has been taken.	X	
Document all issues that arise during the acceptance tests.	X	
Document the results of the acceptance tests and present to the Customer for review.	X	
Resolve any minor task failures before Final System Acceptance.	X	
Deliverable: Completion of functional testing and approval by Customer.		

Tasks	Motorola Solutions	Customer
Training		
Finalize schedule for training coursework.	X	
Provide a training facility.		X
Ensure that the training participants fulfill course prerequisites.		X
Conduct the training classes outlined in the Training Plan.	X	
Attend proposed training classes.		X
Deliverable: Training coursework completed.		
Cutover		
Finalize Cutover Plan.	X	X
Calibrate and tune existing mobile and portable radios to ensure good working order.		X
Provide Motorola Solutions with user radio information for input into the system database and activation, as required.		X
Provide programming of user radios and related services (i.e. template building, re-tuning, testing and installations), as needed, during cutover period.		X
Conduct a cutover meeting with relevant personnel to address both how to mitigate technical and communication problem impacts to the users during cutover and during the general operation of the system.	X	
Notify the personnel affected by the cutover of the date and time planned for the cutover.		X
Provide ongoing communication with users regarding the project and schedule.	X	X
Cut over users and ensure that user radios are operating on the system.		X
Resolve punch list items, documented during the Acceptance Testing phase, in order to meet all the criteria for final system acceptance.	X	
Assist Motorola Solutions with resolution of identified punch list items by providing support, such as access to the sites, equipment and system, and approval of the resolved punch list items.		X
Deliverable: Migration to new system completed, and punch list items resolved.		
Transition to Warranty		
Review the items necessary for transitioning the project to warranty support and service.	X	
Motorola Solutions to provide services during year 1 warranty which align with the proposed services.	X	

Tasks	Motorola Solutions	Customer
Provide a Customer Support Plan detailing the warranty support associated with the contract equipment.	X	
Participate in the Transition Service/Project Transition Certificate (PTC) process.		X
Deliverable: Service information delivered and approved by Customer		
Finalize Documentation and System Acceptance		
Provide manufacturer's installation material, part list and other related material to Customer upon project completion.	X	
Provide an electronic as-built system manual on CD or other Customer preferred electronic media. The documentation will include the following: ▪ Site Block Diagrams. ▪ Site Floor Plans. ▪ Site Equipment Rack Configurations. ▪ Antenna Network Drawings for RF Sites (where applicable). ▪ ATP Test Checklists. ▪ Functional Acceptance Test Plan Test Sheets and Results. ▪ Equipment Inventory List. ▪ Console Programming Template (where applicable). ▪ Maintenance Manuals (where applicable). ▪ Technical Service Manuals (where applicable). ▪ Drawings will be delivered in Adobe PDF format.	X	
Receive and approve documentation.		X
Execute Final Project Acceptance.	X	X
Deliverable: All required documents are provided and approved. Final Project Acceptance.		

4.2 Assumptions

Motorola Solutions has made several assumptions in preparing this proposal, which are noted below. Motorola will need to seek alternate solutions in the case of invalid assumptions.

- A Performance Bond is not required.
- Union Labor is not required.
- Prevailing Wages are not required.
- All existing sites or equipment locations will have sufficient space available for the system described as required/specified by R56.
- All existing sites or equipment locations will have adequate electrical power in the proper phase and voltage, and site grounding to support the requirements of the system described.
    - Electrician services are not included.
    - AC power is assumed on site, no electrical converting equipment is included.

- Any site/location upgrades or modifications are the responsibility of the Customer.
- All Communication Sites can be accessed with a 4 wheel drive vehicle. Anything beyond the use of a 4 wheel drive vehicle will require a change order to capture the additional cost.
- Interfacing to 3rd party equipment or applications is not a part of this proposal.
- Approved FCC licensing is responsibility of the Customer.
- Approved local, State, or Federal permits as may be required for the installation and operation of the proposed equipment are the responsibility of the Customer.
- Any required system interconnections not specifically outlined here will be provided by the Customer. This may include dedicated phone circuits, microwave links, or other types of connectivity.
- Portable and mobiles used for coverage survey or testing will be provided by Customer.
- Training is included in this proposal.
- Motorola Solutions is not responsible for interference caused or received by the Motorola Solutions-provided equipment except for interference that is directly caused by the Motorola Solutions-provided transmitter(s) to the Motorola Solutions-provided receiver(s). Should the Customer's system experience interference, Motorola Solutions can be contracted to investigate the source and recommend solutions to mitigate the issue.
- Backhaul connection to the ORION core is the responsibility of the Fremont Police Department.
- The system is designed to be deployed on an ASTRO System Release 2022.1.
- No new logging recorder has been quoted in this proposal.
- No new antenna systems will be provided for consolette radios and any conventional resources that are moved to the new dispatch center.

Section 5

Infrastructure Essential Plus Services for Federal and Non-Federal Support Description

5.1 Overview

Essential Plus Services for ASTRO® 25 infrastructure will provide City of Fremont with the support needed to detect and resolve unforeseen issues. Essential Plus Services consist of the following elements:

- Remote Technical Support.
- Network Hardware Repair with Advanced Replacement.
- Security Update Service (SUS).
- On-site Infrastructure Response.
- Annual Preventive Maintenance.
- Network Event Monitoring.

Together, these elements will help to avoid operational disruptions and maintain the value of City of Fremont's communications investment.

5.2 Essential Plus Element Descriptions

The following sections describe the elements proposed for City of Fremont's ASTRO 25 infrastructure.

5.2.1 Remote Technical Support

Motorola Solutions' Centralized Managed Support Operations (CMSO) will provide Remote Technical Support for infrastructure issues that require specific technical expertise. Experienced technical support specialists will be available to consult with City of Fremont to help diagnose, troubleshoot and resolve infrastructure issues. Service Desk maintenance procedures and incident resolution techniques are based on ISO 9001 and TL 9000 standards.

5.2.2 Network Hardware Repair with Advanced Replacement

To restore City of Fremont's ASTRO 25 network components if they malfunction, Motorola Solutions will repair Motorola Solutions-provided infrastructure equipment. This includes select third-party infrastructure equipment supplied by Motorola Solutions. Motorola Solutions will ship and return repaired equipment, and will coordinate the repair of third-party solution components.

To reduce the impact of a malfunction, Motorola Solutions will exchange malfunctioning equipment with Advanced Replacement units or Field Replacement Units (FRU), as available. Motorola Solutions' repair depot will diagnose and repair malfunctioning components, and once repaired, add those to the depot's FRU inventory. Replacement components will remain in City of Fremont's ASTRO 25 network to maintain continued network functionality.

If City of Fremont prefers to maintain their existing FRU inventory rather than using Motorola Solutions' depot inventory, Motorola Solutions can provide "loaner" FRUs during the repair process.

5.2.3 Security Update Service

Commercial security software updates are often designed without consideration for specialized systems like radio communications networks. Therefore, they may at sometimes inadvertently disrupt ASTRO 25 networks such as the one proposed to City of Fremont. Motorola Solutions will test anti-virus, operating system and other software patches to check their compatibility with ASTRO 25.

Once tested, Motorola Solutions will post the updates to a secured extranet website and send an email notification to City of Fremont. If there are any recommended configuration changes, warnings or workarounds, Motorola Solutions will provide detailed documentation along with the updates on the website. When tested updates have been posted, City of Fremont will need to download and install them.

5.2.4 On-site Infrastructure Response

Motorola Solutions will provide repair service from trained and qualified technicians. Once dispatched, technicians will travel to City of Fremont's ASTRO 25 network location to diagnose issues and restore functionality. These technicians will run diagnostics on hardware to identify defective components, and repair or replace them as appropriate. Infrastructure Response times are based on a given issue's impact on overall system function.

Travel times and service levels are governed by local geography. Motorola Solutions will provide additional information in the Statement of Work for ASTRO 25 Essential Plus Services and in the Customer Support Plan agreed between City of Fremont and Motorola Solutions.

5.2.5 Annual Preventive Maintenance

Motorola Solutions will annually test and service network components. Qualified field technicians will perform routine hands-on examination and diagnostics of network equipment to keep them operating according to original manufacturer specifications.

5.2.6 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.

5.3 Motorola Solutions Service Delivery Ecosystem

Essential Plus Services are delivered through a tailored combination of field service personnel, centralized teams, product repair depots and Customer Hub. These service resources will collaborate to swiftly analyze network issues, accurately diagnose root causes, and efficiently resolve issues to return the network to normal operation.

Motorola Solutions services will be delivered by staff experienced in servicing mission-critical networks. Motorola Solutions uses the Information Technology Infrastructure Library (ITIL) framework to define service tasks based on industry-recognized best practices. As staff perform tasks, service incident information will be available to City of Fremont's administrators and personnel through Customer Hub.

Service activities and Motorola Solutions' service team are described in more detail below.

5.3.1 Centralized Managed Support Operations

The cornerstone of Motorola Solutions' support process is the Centralized Managed Support Operations (CMSO) organization. This TL 9000/ISO 9001-certified organization is staffed 24x7x365 by experienced service desk specialists, security analysts and operations managers. The CMSO houses critical central functions, including the Service Desk.

The CMSO Service Desk will serve as a single point of contact for services. It processes service requests, service incidents, change requests, and dispatching. The Service Desk communicates necessary information to stakeholders, bridging communications among City of Fremont, Motorola Solutions, and third-party subcontractors.

Service Desk teams record, track, and update incidents through the Motorola Solutions Customer Relationship Management (CRM) system. They document and respond to inquiries, requests, concerns and service tickets. When an incident is initiated, the CMSO will engage with teams to resolve that incident. The CMSO will escalate to new teams when needed. Depending on the incident, the CMSO will coordinate incident resolution with local field service and authorized repair depots.

5.3.2 Field Service

Motorola Solutions authorized and qualified field service technicians will perform the On-site Infrastructure Response service, repair malfunctioning hardware in the field, and conduct preventive maintenance tasks. These technicians will coordinate with the Service Desk, technical support teams, and product engineering as needed to resolve incidents.

5.3.3 Repair Depot

The Motorola Solutions Repair Depot will provide City of Fremont with a central repair location. This will eliminate the need to send network equipment to multiple vendor locations for repair. Motorola Solutions tracks products sent to the Depot via a case management system throughout the repair process. This system will enable City of Fremont's representatives to check repair status, from inbound shipment to return.

5.3.4 Customer Support Manager

A Motorola Solutions Customer Support Manager (CSM) will be City of Fremont's key point of contact for the definition and administration of services. The CSM will work with City of Fremont to define service delivery details to address City of Fremont's specific priorities.

5.3.5 Customer Hub

To provide City of Fremont with quick access to service details, Motorola Solutions will provide our Customer Hub online network information tool. Customer Hub provides our customers with real-time critical network and services information through an easy-to-use graphical interface.

Customer Hub offers real-time, role-based access to critical network and services information.

With Customer Hub, City of Fremont's administrators will be able to monitor system health and maintenance updates. Capabilities include:

- Viewing network and support compliance.
- Viewing incident reports.
- Updating and creating incidents.
- Checking system update status.
- Receiving pro-active notifications regarding updates.

Available 24x7x365 from any web-enabled device, the information provided by Customer Hub will be based on your needs and user access permissions, ensuring that the information displayed is secure and pertinent to your operations.

Section 6

ASTRO 25 Essential Plus Statement of Work

6.1 Overview

Motorola Solutions' ASTRO® 25 Essential Plus Services (Essential 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. Essential Services do not include maintenance for mobile devices, portable devices, or network backhaul equipment.

Essential Services consist of the following elements:

- Remote Technical Support.
- Network Hardware Repair.
- Security Update Service.
- On-site Infrastructure Response.
- Annual Preventative Maintenance.
- Network Event Monitoring

Each of these elements is summarized below and expanded upon in Section Essential Plus Services Detailed Description. In the event of a conflict between the descriptions below and an individual subsection of Section Essential 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 Solutions, Inc. (Motorola Solutions) and the customer (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 Solutions' Software Support Policy (SwSP).

6.1.1.1.1 *Remote Technical Support*

Motorola Solutions 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.

6.1.1.1.2 *Network Hardware Repair*

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

6.1.1.1.3 *Security Update Service*

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

6.1.1.1.4 *On-site Infrastructure Response*

When needed to resolve equipment malfunctions, Motorola Solutions 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.

6.1.1.1.5 *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.

6.1.1.1.6 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.

6.2 Motorola Solutions Service Delivery Ecosystem

Essential 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.

6.2.1 Centralized Managed Support Operations

The cornerstone of Motorola Solutions' support process is the Centralized Managed Support Operations (CMSO) organization, which includes the Service Desk and technical support teams. The CMSO is staffed 24/7/365 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 Solutions, and third-party subcontractors. The Service Desk processes service requests, service incidents, change requests, and dispatching, and communicates with stakeholders in accordance with pre-defined response times.

All incoming transactions through the Service Desk are recorded, tracked, and updated through the Motorola Solutions 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.

6.2.2 Field Service

Motorola Solutions 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.

6.2.3 Customer Support Manager

A Motorola Solutions 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 Solutions 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 Statement of Work 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 Essential Services.

6.2.4 Repair Depot

The Motorola Solutions Repair Depot provides the Customer with a central repair location, eliminating the need to send network equipment to multiple vendor locations for repair. All products sent to the Depot are tracked throughout the repair process, from inbound shipment to return, through a case management system that enables Customer representatives to see repair status.

6.2.5 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:

- **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 Solutions' 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.
- **Security Update Service**: View available security updates. Access available security update downloads.
- **On-site Infrastructure Res**ponse: 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.
- **Orders and Contract Information**: View available information regarding orders, service contracts, and service coverage details.
- **Network Event Monitoring**: Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.

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.

6.2.6 Connectivity Specifications

A monitored access link is provided with sufficient bandwidth to support the optional Network Event Monitoring and Remote Security Update Services, if included as part of the Essential Plus offering.

6.3 Essential 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.

6.3.1 Remote Technical Support

Motorola Solutions' 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 Solutions CMSO organization by a staff of technical support specialists skilled in diagnosis and swift resolution of infrastructure performance and operational issues.

Motorola Solutions 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.

6.3.1.1 Description of Service

The CMSO organization's primary goal is Customer Issue Resolution (CIR), providing incident restoration and service request fulfillment for Motorola Solutions' 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 Solutions' CRM system, and Motorola Solutions 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 Solutions 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 Priority Level Definitions and Response Times.

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

6.3.1.2 Scope

The CMSO Service Desk is available via telephone 24/7/365 to receive and log requests for technical support. Remote Technical Support service is provided in accordance with Section Priority Level Definitions and Response Times.

6.3.1.3 Inclusions

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

6.3.1.4 Motorola Solutions Responsibilities

- Maintain availability of the Motorola Solutions CMSO Service Desk via telephone (800-MSI-HELP) 24/7/365 to receive, log, and classify Customer requests for support.
- Respond to incidents and technical service requests in accordance with Section Priority Level Definitions and Response Times.
- Provide caller a plan of action outlining additional requirements, activities, or information required to achieve restoral/fulfillment.
- Maintain communication with the Customer in the field as needed until resolution of the incident.
- Coordinate technical resolutions with agreed upon third-party vendors, as needed.
- Escalate support issues to additional Motorola Solutions 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.

6.3.1.5 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 Solutions.
- Any maintenance and/or remediation required as a result of a virus or unwanted cyber intrusion.

6.3.1.6 Customer Responsibilities

- Prior to contract start date, provide Motorola Solutions 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 Priority Level Definitions and Response Times.
- Cooperate with Motorola Solutions, and perform all acts that are reasonable or necessary to enable Motorola Solutions to provide Remote Technical Support.
- In the event that Motorola Solutions 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 Solutions to provide the service.

6.3.2 Network Hardware Repair with Advanced Replacement

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

6.3.2.1 Description of Service

Infrastructure components are repaired at Motorola Solutions-authorized Infrastructure Depot Operations (IDO). At Motorola Solutions' 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.

6.3.2.2 Scope

Repair authorizations are obtained by contacting the CMSO organization Service Desk, which is available 24/7/365. Repair authorizations can also be obtained by contacting the CSM.

6.3.2.3 Inclusions

This service is available on Motorola Solutions-provided infrastructure components, including integrated third-party products. Motorola Solutions will make a commercially reasonable effort to repair Motorola Solutions 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.

6.3.2.4 Motorola Solutions 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 Solutions infrastructure:
    - Perform an operational check on infrastructure components to determine the nature of the problem.
    - Replace malfunctioning components.
    - Verify that Motorola Solutions infrastructure components are returned to applicable Motorola Solutions 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 Solutions system configuration.
- Reprogram repaired infrastructure components to original operating parameters based on software and firmware provided by the Customer, as required in Section 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 Solutions 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.

6.3.2.5 Limitations and Exclusions

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

- All Motorola Solutions infrastructure components over the post-cancellation support period.
- All third-party 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 Solutions.
- 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, dropship non-standard items and test equipment.
- Racks, furniture, and cabinets.
- Non-standard configurations, customer-modified infrastructure, and certain third party infrastructure.
- Firmware or software upgrades.

6.3.2.6 Customer Responsibilities

- Contact or instruct servicer to contact the Motorola Solutions 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 Solutions or third-party infrastructure components being sent in for service were subjected to physical damage or lightning damage.
- Follow Motorola Solutions 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 Solutions 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 Solutions with proper software and firmware information to reprogram equipment after repair, unless current software has caused this malfunction.
- Cooperate with Motorola Solutions and perform reasonable or necessary acts to enable Motorola Solutions to provide hardware repair services to the Customer.
- At the Customer's cost, obtain all third-party consents or licenses required to enable Motorola Solutions to provide the service.

6.3.2.7 Repair Process

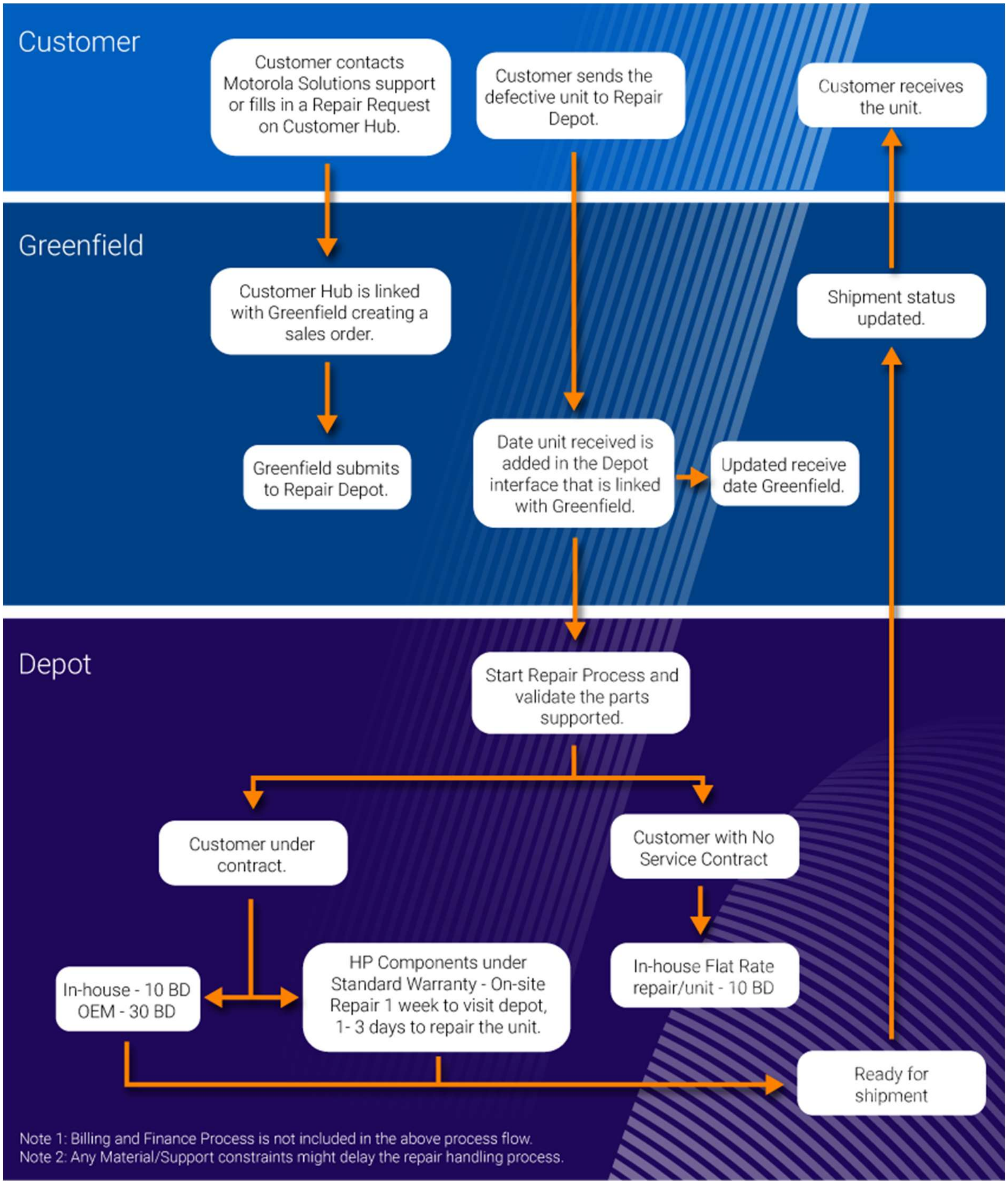

Customer
Customer contacts Motorola Solutions support or fills in a Repair Request on Customer Hub.
Customer sends the defective unit to Repair Depot.
Customer receives the unit.
Greenfield
Customer Hub is linked with Greenfield creating a sales order.
Greenfield submits to Repair Depot.
Date unit received is added in the Depot interface that is linked with Greenfield.
Updated receive date Greenfield.
Shipment status updated.
Depot
Start Repair Process and validate the parts supported.
Customer under contract.
Customer with No Service Contract
In-house - 10 BD
OEM - 30 BD
HP Components under Standard Warranty - On-site Repair 1 week to visit depot, 1- 3 days to repair the unit.
In-house Flat Rate repair/unit - 10 BD
Ready for shipment
Note 1: Billing and Finance Process is not included in the above process flow.
Note 2: Any Material/Support constraints might delay the repair handling process.

Figure 1-1: Repair Decision Process

6.3.2.8 Advanced Replacement

As an addition to Hardware Repair service, Advanced Replacement is a repair exchange service for Motorola Solutions and select third-party infrastructure components supplied by Motorola Solutions. When available, Motorola Solutions will provide the Customer with advanced replacement units or Field

Replacement Units (FRU) in exchange for the Customer's malfunctioning equipment. A Motorola Solutions-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 1-2: Advanced Replacement Decision Process for details on the unit loan process.

6.3.2.8.1 Added Motorola Solutions Responsibilities for Advanced Replacement

- Use commercially reasonable efforts to maintain FRU inventory on supported platforms.
- Provide new or reconditioned FRUs to the Customer upon request, 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 Solutions 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 Solutions 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 Solutions 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.

6.3.2.8.2 Added Customer Responsibilities for Advanced Replacement

- Pay for Advanced Replacement FRU shipping from Motorola Solutions repair depot if the Customer requested shipping outside of standard business hours or carrier programs set forth in Section On-site Delivery. See Table 1-1: 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 Solutions' FRU inventory, properly package the Customer's malfunctioning FRU and ship the malfunctioning Infrastructure to Motorola Solutions' 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 FRUs not returned within five business days.
- At the Customer's expense and risk of loss, the Customer may send a malfunctioning Motorola Solutions 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 Solutions.
- Clearly print the return authorization number on the outside of the packaging.

6.3.2.8.3 Replacement Process for Advanced Replacement

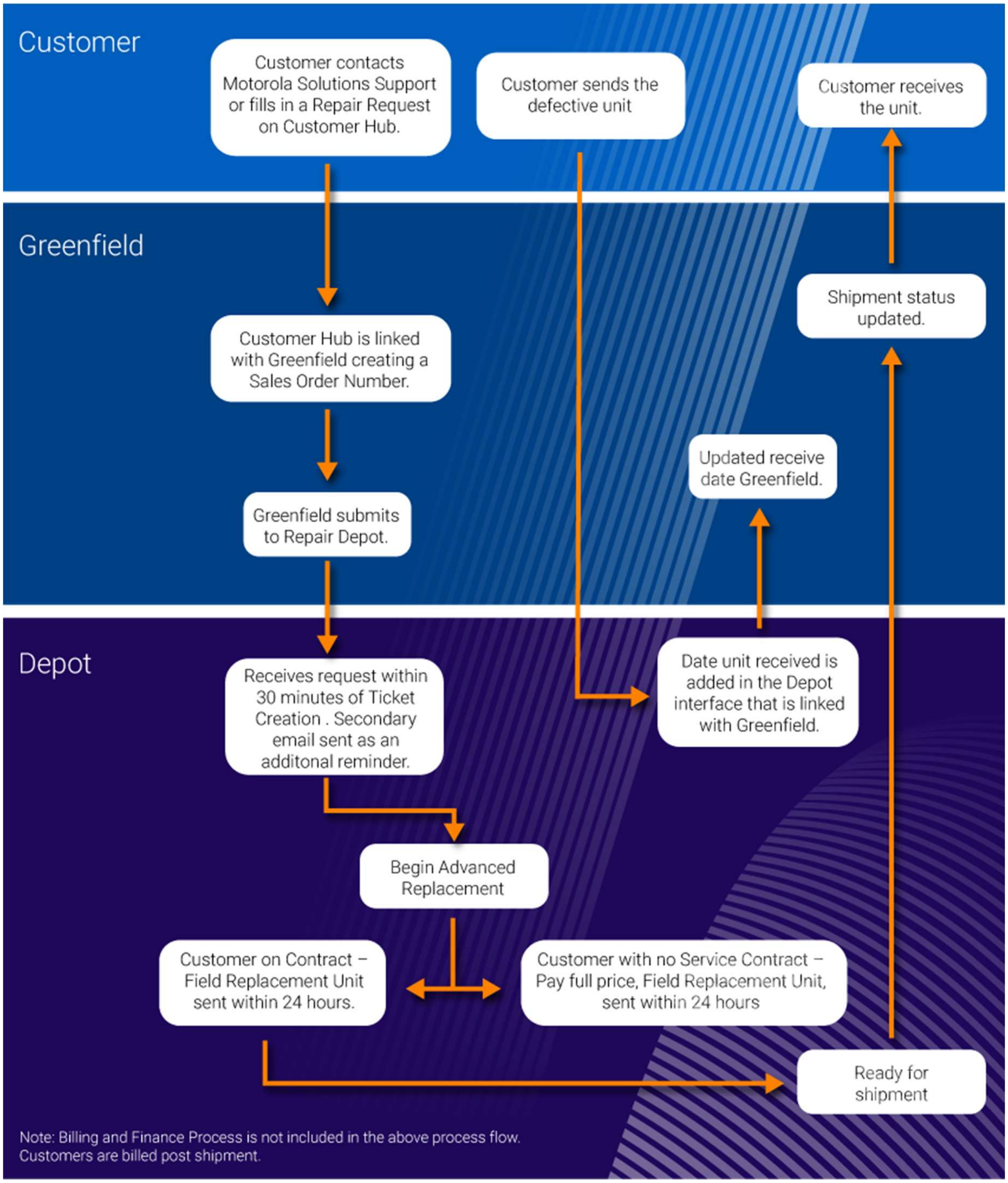

Customer
Customer contacts Motorola Solutions Support or fills in a Repair Request on Customer Hub.
Customer sends the defective unit
Customer receives the unit.
Greenfield
Shipment status updated.
Customer Hub is linked with Greenfield creating a Sales Order Number.
Updated receive date Greenfield.
Greenfield submits to Repair Depot.
Depot
Receives request within 30 minutes of Ticket Creation . Secondary email sent as an additonal reminder.
Date unit received is added in the Depot interface that is linked with Greenfield.
Begin Advanced Replacement
Customer on Contract – Field Replacement Unit sent within 24 hours.
Customer with no Service Contract – Pay full price, Field Replacement Unit, sent within 24 hours
Ready for shipment
Note: Billing and Finance Process is not included in the above process flow. Customers are billed post shipment.

Figure 1-2: Advanced Replacement Decision Process

6.3.2.8.4 *Replacement Process for Advanced Replacement*

Table 1-1: Shipping Charges and Default Mail Service

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

Motorola Solutions shipping carrier: FedEx

6.3.3 Security Update Service

Motorola Solutions' 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 Inclusions indicates if options are included as part of this service.

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 Solutions' Software Support Policy (SwSP).

6.3.3.1 Description of Service

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

Motorola Solutions releases tested, compatible security updates for download and installation. Once security updates are verified by the SUS team, Motorola Solutions 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.

With the base 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 Solutions to deploy security updates, reboot servers and workstations, or both.

6.3.3.1.1 On-site Delivery

If On-site Delivery is included with SUS, Motorola Solutions 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. On-Site delivery is not available for the optional transport network updates for routers, firewalls and switches. If on-site transport network updates are required please discuss this with your Motorola Solutions Customer Support Manager.

6.3.3.1.2 *Reboot Support*

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

6.3.3.2 Scope

SUS includes pretested security updates for the software listed in Table 1-2: Update Cadence. This table also describes the release cadence for security updates.

Table 1-2: 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 (A2024 or earlier only)	Quarterly
PostgreSQL	Quarterly
Antivirus Software Patch(es)	Quarterly
Server Firmware Updates	Quarterly
QNAP Firmware	Quarterly
Juniper Firewall Updates	Bi-Annually*
Juniper Router Updates	Bi-annually*
Fortinet Firewall Updates	As required - no regular cadence*
Juniper Switch Updates	As required - no regular cadence*
Aruba Switch Updates	As required - no regular cadence*

**To receive the updates for ASTRO Transport Network devices, the Customer is required to "Opt-In". Please see Section 1.4 below.*

6.3.3.3 Transport Network Updates

Updates to the transport network devices, which includes routers, firewalls and switches, will be issued up to twice a year (subject to applicability of vendor updates). See Table 1.

These updates require customer specific network device configurations which can only be prepared by Motorola Solutions.

6.3.3.3.1 Opt-In

To receive configuration files for updating their transport network devices, customers must actively choose to "Opt-In."

If customers choose to perform these updates themselves, it will involve a certain level of interaction and shared responsibilities between the customer and Motorola Solutions.

The customer's decision and requirements for opting in are documented during the initial service onboarding process.

6.3.3.3.2 Configuration Files

When Customers "Opt-In", their assigned Motorola Solutions engineer will provide any network configuration file updates needed for Customers to self-deploy the new device software release.

6.3.3.3.3 Deployment Options

The download and installation of the transport network updates are the responsibility of the Customer, with remote support from Motorola to provide configuration file updates.

An alternative option available, should the Customer require Motorola Solutions to deploy the updates, is an onsite deployment service, which is quoted separately. Please discuss this with your CSM.

Note that transport network updates are not included in the ASTRO 25 Remote Security Update Service.

6.3.3.3.4 Change Management

Customers are required to notify Motorola Solutions prior to deploying the updates (by calling the service desk). Your assigned MSI engineer who is supporting you with configuration changes will also raise/close the necessary Change Requests using the Motorola Solutions Change Management process.

6.3.3.4 Inclusions

Supported ASTRO 25 core types and security update delivery methods are included in Table 1-3: SUS Package. This table indicates if Motorola Solutions will provide any SUS optional services to the Customer. SUS supports the current Motorola Solutions ASTRO 25 system release and aligns with the established Software Support Policy (SwSP).

Motorola Solutions 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 Solutions' assigned CSM for the latest supported releases.

Table 1-3: SUS Package

Service	ASTRO 25 Core Type	Included
Security Update Service Customer Self-installed	Standard Core Simplified Core	X
Security Update Service Customer Self-installed (Transport Network Updates)*	Standard Core Simplified Core	

Service	ASTRO 25 Core Type	Included
Security Update Service with Reboot Support	Standard Core Simplified Core	
Security Update Service with On-site Delivery	Standard Core Simplified Core	

**To receive the updates for ASTRO Transport Network devices, the Customer is required to "Opt-In". Please see Section 1.4.*

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

6.3.3.5 Motorola Solutions Responsibilities

- On the release schedule in Section Scope, review relevant and appropriate security patches released by Original Equipment Manufacturer (OEM) vendors.
- Release tested and verified security patches to Motorola Solutions' 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.
- For Customers who opt in to receive Transport Network Device Updates (Routers, Firewalls, Switches), Motorola Solutions shall:
  - Coordinate with the Customer to determine when Transport Network Configuration Tool (TNCT) files need to be updated.
  - Coordinate the retrieval of the current TNCT configurations from the Customer's system.
  - Update TNCT files (where applicable) to ensure compatibility with updated device software.
  - Coordinate the deposit of the updated configurations to the Customer's system (prior to the Customer's planned update deployment activity).

6.3.3.6 Limitations and Exclusions

- Systems with non-standard configurations that have not been certified by Motorola Solutions' Systems Integration and Test (SIT) team are specifically excluded from this service, unless otherwise agreed in writing by Motorola Solutions.
- Interim or unplanned releases outside the supported release cadence.
- Service does not include pretested intrusion detection system (IDS) signature updates for IDS solutions. However, select vendor IDS signature updates are made available via the secure website. The available vendors may change pursuant to Motorola Solutions' business decisions. The Customer is responsible for complying with all IDS licensing requirements and fees, if any.

- This service does not include releases for Motorola Solutions products that are not ASTRO 25 Standard 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 Solutions product updates are not included in these services.
- Shared network infrastructure firmware, such as transport and firewall firmware, are not included in these services, unless the Customer has opted-in to deploy them and receive configuration support.
- Workstation firmware, BIOS and drivers are not included in these services.
- Motorola Solutions 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.

6.3.3.7 Customer Responsibilities

- Provide Motorola Solutions 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 Solutions' assigned CSM.
- Update Motorola Solutions with any changes in contact information, specifically for authorized users of Motorola Solutions' secure website.
- Provide means for accessing Motorola Solutions' 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 CMSO troubleshooting guidelines provided upon system acquisition. Failure to follow CMSO guidelines may cause the Customer and Motorola Solutions unnecessary or overly burdensome remediation efforts. In such cases, Motorola Solutions 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 Solutions' assigned CSM for the latest supported releases.
- For Customers who opt in to receive Transport Network Device Updates (Routers, Firewalls, Switches), the Customer shall:
  - Provide required information regarding the Customer's planned deployment schedule, including proposed update period.
  - Coordinate with Motorola Solutions engineers to provide current network configuration files.
  - Coordinate with Motorola Solutions to upload replacement configuration files (where applicable).

- ○ Provide the information necessary for to raise a Change Request to cover the period of the transport network update activity prior to deployment of updates.
- ○ Notify Motorola Solutions when updates are completed.

- Comply with the terms of applicable license agreements between the Customer and non-Motorola Solutions software copyright owners.

6.3.3.8 Installation and Reboot Responsibilities

Installation and Reboot responsibilities are determined by the specific SUS package being purchased. Table 1-4: Installation and Reboot Responsibilities Matrix contains the breakdown of responsibilities. Section 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 1-4: Installation and Reboot Responsibilities Matrix

SUS Package	Motorola Solutions Responsibilities	Customer Responsibilities
Security Update Service Customer Self-installed		● Deploy pretested files to the Customer's system as instructed in the "Read Me" text provided on Motorola Solutions' secure website. ● When a security update requires a reboot, reboot servers and workstations after security updates are installed.
Customer Self-installed with Transport Network Opt-In	● Update TNCT configurations for compatibility with device updates ● Raise Change requests prior to deployment of updates ● Close Change requests on completion of updates	● Deploy files to the Customer's system as instructed in the installation procedures provided on Motorola Solutions' secure website. ● Deploy updates and restart devices (where applicable)
Security Update Service with On-site Delivery	● Dispatch a technician to deploy pretested files to the Customer's system. ● When a security update requires a reboot, reboot servers and workstations after security updates are installed.	● Acknowledge Motorola Solutions will reboot servers and workstations, and agree to timing.

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

6.3.3.9 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 Solutions 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 Solutions. Motorola Solutions 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 Solutions 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 Solutions disclaims any warranty concerning non-Motorola Solutions software and does not guarantee Customers' systems will be error-free or immune to security breaches as a result of these services.

Additionally, Customers who opt-in to receive configuration files for updating their transport network devices, and that elect to self-install those updates, understand and agree to accept responsibility for and the risks associated with self-installation, which may include service interruptions or system downtime.

6.3.4 On-site Infrastructure Response

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

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

6.3.4.1 Description of Service

The Motorola Solutions 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 Priority Level Definitions and Response Times.

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

6.3.4.2 Scope

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

6.3.4.3 Geographical Availability

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

6.3.4.4 Inclusions

On-site Infrastructure Response is provided for Motorola Solutions-provided infrastructure.

6.3.4.5 Motorola Solutions 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 Solutions' standard procedures, and provide necessary incident information.
- Provide the required personnel access to relevant Customer information, as needed.
- Motorola Solutions 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 Solutions 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 Solutions field service technician, arrival of the field service technician on-site, delayed, or closed.
- Provide incident activity reports to the Customer, if requested.

6.3.4.6 Limitations and Exclusions

The following items are excluded from this service:

- All Motorola Solutions 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 Solutions.
- 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.

6.3.4.7 Customer Responsibilities

- Contact Motorola Solutions, as necessary, to request service.
- Prior to start date, provide Motorola Solutions 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 Solutions to open an incident.
- Provide field service technician with access to equipment.
- Supply infrastructure spare or FRU, as applicable, in order for Motorola Solutions 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 Solutions and perform reasonable or necessary acts to enable Motorola Solutions to provide these services.
- In the event that Motorola Solutions 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 Solutions to provide the service.

6.3.4.8 Priority Level Definitions and Response Times

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

Table 1-6: Standard Level Definitions and Response Times

Incident Priority	Incident Definition	On-site Response Time
Critical P1	**Core**: Core server or core link failure. No redundant server or link available. **Sites/Subsites**: Primary site down. Two RF sites or more than 10% of RF sites down, whichever is greater. **Consoles**: More than 40% of a site's console positions down. **Conventional Channels**: Conventional Channel Gateways (CCGW) down without redundant gateways available. **Security Features**: Security is non-functional or degraded.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.

Incident Priority	Incident Definition	On-site Response Time
High P2	**Core**: Core server or link failures. Redundant server or link available. **Consoles**: Between 20% and 40% of a site's console positions down. **Sites/Subsites**: One RF site or up to 10% of RF sites down, whichever is greater. **Conventional Channels**: Up to 50% of CCGWs down. Redundant gateways available. **Network Elements**: Site router, site switch, or GPS server down. No redundant networking element available.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
Medium P3	**Consoles**: Up to 20% of a site's console positions down. **Conventional Channels:** Single channel down. Redundant gateway available. **Network Elements**: Site router/switch or GPS server down. Redundant networking element available.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 8 hours of receiving dispatch notification.
Low P4	**Service Requests**: Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).	Not applicable.

Table 1-7: 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.

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 1-8: Limited 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 during normal business hours until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
High P2	**Core**: Core server or link failures. Redundant server or link available. **Consoles**: Between 20% and 40% of a site's console positions down. **Sites/Subsites**: One RF site or up to 10% of RF sites down, whichever is greater. **Conventional Channels**: Up to 50% of CCGWs down. Redundant gateways available. **Network Elements**: Site router, site switch, or GPS server down. No redundant networking element available.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
Medium P3	**Consoles**: Up to 20% of a site's console positions down. **Conventional Channels**: Single channel down. Redundant gateway available. **Network Elements**: Site router/switch or GPS server down. Redundant networking element available.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 8 hours of receiving dispatch notification.
Low P4	**Service Requests**: Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).	Not applicable.

6.3.5 Annual Preventative Maintenance

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

6.3.5.1 Description of Service

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

6.3.5.2 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.

6.3.5.3 Inclusions

Annual Preventive Maintenance service will be delivered for Motorola Solutions-provided infrastructure, including integrated third-party products, per the level of service marked in Table 1-9: Preventive Maintenance Level.

Table 1-9: Preventive Maintenance Level

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

6.3.5.4 Motorola Solutions 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 Preventative Maintenance Tasks.
    - Perform the procedures defined in Section Site Performance Evaluation Procedures for each site type on the system.

- ○ Provide diagnostic and test equipment necessary to perform the Preventive Maintenance service.
- ○ As applicable, use the Method of Procedure (MOP) defined for each task.

6.3.5.5 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 Solutions 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.

6.3.5.6 Customer Responsibilities

- Provide preferred schedule for Annual Preventative Maintenance to Motorola Solutions.
- 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 Solutions full, free, and safe access to the equipment so that Motorola Solutions 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 Solutions with requirements necessary for access to secure facilities.
- In the event that Motorola Solutions 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 Solutions field service technician to access the sites to provide the service.

6.3.5.7 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 Inclusions.

MASTER SITE CHECKLIST – LEVEL 1	
Servers	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.

MASTER SITE CHECKLIST – LEVEL 1	
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 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 core security management server were updated within two weeks of current date.
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.

MASTER SITE CHECKLIST – LEVEL 1	
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 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.

MASTER SITE CHECKLIST – LEVEL 1	
Server CPU Health	Check memory, HDD, CPU, and disk space utilization.

PRIME SITE CHECKLIST – LEVEL 1	
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 Customer server.
Switches	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on switch type. Capture available diagnostic logs.
Clean Fans and Equipment	Use antistatic vacuum to clean cooling pathways.
Routers	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on router type. Capture available diagnostic logs.
Clean Fans and Equipment	Use antistatic vacuum to clean cooling pathways.
Miscellaneous Equipment	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
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 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 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.
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 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 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.
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 Solutions dispatch (if applicable).
Telephone IRR Operation	Verify telephone IRR operational on Motorola Solutions 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 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 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 Customer server.
Playback Station (Motorola Solutions 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.
Clean Fans and Equipment	Use an antistatic vacuum to clean cooling pathways.
Site Frequency Standard Check	Check LEDs for proper operation,PCA screens indicating potential faults for proper operation
Basic Voice Call Check	Voice test each voice path, radio to radio.
Trunking Control Channel Redundancy	Roll control channel, test, and roll back if the site has GTR stations. This test is not applicable for D series stations.
Trunking Site Controller Redundancy, ASTRO® 25 Site Repeater only	Roll site controllers with no dropped audio if the site has GTR stations.This test is not applicable for D series stations.

RF SITE CHECKLIST – LEVEL 1	
PM Optimization Workbook (See Section 1.3.20.8: Site Performance Evaluation Procedures for GTR tests)	Complete Base Station Evaluation tests - Frequency Error, Modulation Fidelity, Forward at Set Power, Reverse at Set Power, and Gen Level Desense no TX. Update station logs.

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

FACILITIES CHECKLIST – LEVEL 1	
Visual Inspection Exterior	
Antenna Site Registration Sign	Verify that the Antenna Site Registration sign is posted.

FACILITIES CHECKLIST – LEVEL 1	
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 exterior of building for damage and disrepair.
Fences / Gates	Check fences and gates for damage and disrepair.
Landscape / Access Road	Check landscape and access road for accessibility.
Visual Inspection Interior	
Electrical Surge Protectors	Check electrical surge protectors for alarms.
Emergency Lighting	Verify emergency lighting operation.
Indoor Lighting	Verify indoor lighting.
Equipment Inspection	Visually inspect that all hardware, including equipment, cables, panels, batteries, and racks, is in acceptable physical condition for normal operation.
Regulatory Compliance (License, ERP, Frequency, Deviation)	Check for site and station FCC licensing indicating regulatory compliance.
Clean Fans and Equipment	Use antistatic vacuum to clean cooling pathways.
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 proper level. Note condition of oil.
Verify operation (no switchover)	Verify generator running and check ease or difficulty of start. Is 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 outdoor unit is unobstructed.
Wiring	Check wiring for insect and rodent damage.
Cooling / Heating	Check each HVAC unit for cooling/heating.

FACILITIES CHECKLIST – LEVEL 1	
Motorized Dampers	Check operation.

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

6.3.5.8 Site Performance Evaluation Procedures

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

ASTRO 25 SITE PERFORMANCE
Antennas
Transmit Antenna Data
Receive Antenna System Data
Tower Top Amplifier Data

ASTRO 25 SITE PERFORMANCE
FDMA Mode
Base Radio Transmitter Tests
Base Radio Receiver Tests
Base Radio Transmit RFDS Tests
Receive RFDS Tests with TTA (if applicable)
Receive RFDS Tests without TTA (if applicable)
TDMA Mode
Base Radio TDMA Transmitter Tests
Base Radio TDMA Receiver Tests
TDMA Transmit RFDS Tests
TDMA Receive RFDS Tests with 432 Diversity TTA
TDMA Receive RFDS Tests with 2 Independent TTAs (if applicable)
TDMA Receive RFDS Tests without TTA (if applicable)

6.4 Priority Level Definitions and Response Times

Table 1-10: Priority Level Definitions and Response Times describes the criteria Motorola Solutions CMSO uses to prioritize incidents and service requests, and lists the response times for those priority levels.

Table 1-10: Priority Level Definitions and Response Times

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

Incident Priority	Incident Definition	Initial 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. Technical resource will acknowledge incident and respond within 1 Business Day of CMSO logging incident.
Low P4	**Service Requests:** Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).	Response provided during normal business hours. Motorola Solutions will acknowledge and respond within 1 Business Day.

6.5 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.

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 1-11: Alarm Threshold Rule Options for All Event Types.

Table 1-11: Alarm Threshold Rule Options for All Event Types

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

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

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

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

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

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

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

6.5.1 Scope

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

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

6.5.2 Inclusions

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

6.5.3 Motorola Responsibilities

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

- Cooperate with the Customer to coordinate the transition of monitoring responsibilities between Motorola Solutions and the Customer as specified in Section Customer Responsibilities.
- Maintain communication as needed with the Customer in the field until incident resolution.
- Provide available information on incident resolution to the Customer.

6.5.4 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.
- Emergency on-site visits required to resolve technical issues that cannot be resolved by working remotely with the Customer's technical resource.
- Elements deployed outside of ASTRO RNI (e.g., ASTRO CEN sites) are excluded from the service.
- System installations, upgrades, and expansions.
- Customer training.
- Hardware repair and/or replacement.
- Network security services.
- Information Assurance.

6.5.5 Customer Responsibilities

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

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

6.5.6 Connectivity Matrix

ASTRO connectivity should be established prior to service start date.

Table 1-12: Available Connectivity

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

6.5.7 Motorola Solutions Owned and Supplied Equipment

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

Table 1-13: Motorola Solutions Owned and Supplied Equipment

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

6.5.8 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 1-14: 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
Load Balancer	Load Balancer	TRAK
Client Station	Logging Recorder	Terminal Server
CommandCentral AXS Dispatch Console	Logging Replay Station	Time Keeper
Controller	UNC	Training App
Conventional	UEM	Training Database
Core Router	MOSCAD Server	Trap Forwarder
Data Processing	Network Address	UCS
Database Server	Network Device	Licensing Server
Data Warehouse Server	NTP	Virtual Machine
Device Configuration Server	AIS	VMS
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

Monitored Elements		
Repeaters	Power Monitor	Proxy

Section 7

ASTRO® System Upgrade Agreement Statement of Work

7.1 Overview

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

Motorola Solutions, Inc. (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).

7.2 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 1: SUA Term**. The eligible System Upgrade windows and their duration are illustrated in **Table 2: Eligible System 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 2: Eligible System 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.

Table 1: SUA Term

Duration	5 Years

Table 2: Eligible System Upgrade Window

First Eligible Upgrade Window	Second Eligible Upgrade Window	Third Eligible Upgrade Window
Duration: TBD	Duration: TBD	Duration: TBD

The methodology for executing each System Upgrade is described in Section 1.5**. 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.

7.3 Inclusions

Refer to Table C-6: SUA Coverage Table for more detailed information on the SUA inclusions referenced in this section.

7.3.1 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.

7.3.2 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 1.4.5 for further clarification on coverage.

7.4 Limitations and Exclusions

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

Excluded Products and Services	Examples (Not Limited To)
Purchased directly from a third party	NICE, Genesis, Verint
Residing outside of the ASTRO® network	CAD, E911, Avtec Consoles
Not certified on ASTRO® systems	Laptops, PCs, Eventide loggers

Excluded Products and Services	Examples (Not Limited To)
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, Multicouplers
Customer-provided cloud connectivity	LTE, Internet
Maintenance Services of any kind	Infrastructure Repair, Tech Support, Dispatch
Security Services	Security Update Service (SUS), Remote SUS

7.4.1 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.

7.4.2 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.

7.4.3 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.

7.4.4 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.

7.4.5 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.

7.5 General Statement of Work for System Upgrades

7.5.1 Upgrade Planning and Preparation

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

7.5.1.1 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.

7.5.1.2 Customer Responsibilities

- 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 1.5.1.1 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 1.5.1.1 Motorola Responsibilities. 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.

7.5.2 System Readiness Checkpoint

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

7.5.2.1 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.

7.5.2.2 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.

7.5.3 System Upgrade

7.5.3.1 Motorola Responsibilities

- Perform System Upgrade for the system elements outlined in this SOW.

7.5.3.2 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.

7.5.4 Upgrade Completion

7.5.4.1 Motorola Responsibilities

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

7.5.4.2 Customer Responsibilities

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

7.6 Special Provisions

The migration of capabilities from ASTRO® on-premises Core infrastructure to the cloud is 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 a System 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 is responsible for 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's 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® SUA coverage and the parties’ responsibilities described in this SOW will automatically terminate if Motorola no longer supports the ASTRO® 7.x software version in the Customer’s system or discontinues the ASTRO® SUA program. In either case, Motorola will refund to Customer any prepaid fees for ASTRO® 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® SUA annualized price is based on the fulfillment of the system release upgrade in each eligible System 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 System Upgrade window if a system release upgrade has been taken prior to the point of termination.

7.7 Appendix A: ASTRO® System Release Upgrade Paths

The upgrade paths for standard ASTRO® system releases are listed in **Table A-3: Certified Standard ASTRO® System Release Upgrade Paths.**

Table A-3: Certified Standard ASTRO® System Release Upgrade Paths

ASTRO® 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-4: Certified High Security ASTRO® System Release Upgrade Paths**.

Table A-4: Certified High Security ASTRO® System Release Upgrade Paths

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

The release taxonomy for the ASTRO® 7.x platform is expressed in the form "ASTRO® 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® System release with support for Public Key Infrastructure (PKI) Common Access Card / Personal Identity Verification (CAC/PIV) and with Cyber Security Baseline Assurance.

Starting with the 2024 releases, Motorola is moving from the ASTRO 7.x release names to ASTRO Next. For the purposes of the SUA program, releases using the naming convention of AN (ASTRO Next) or A (ASTRO) will be considered the same.

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

7.8 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.

Table B-5: System Configuration at Time of Contract

System Configuration	
Core Configuration	
Cloud-based Core	0
On-premises Main Site	0
On-premises Backup Site	0
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 Configuration	
AERSS Sensors	0
Firewalls	0
KMF Servers	0
KMF Clients	0
RF Site Configuration	
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
DBR 8000 Base Stations	0
Dispatch Site Configuration	
Dispatch Site Locations	0
MCC 7500 Dispatch Consoles	0
AIS	0

System Configuration	
CCGWs	1
MC EDGE Aux I/O	0
AXS Console Dispatch Site Locations	1
AXS Console PDH (CommandCentral Hub)	6
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

7.9 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-6: 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)	✓	✓	

ASTRO® Certified Solution	System Upgrade		
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)	✓	✓	

Section 8

Pricing Summary

8.1 Pricing

Description	Price ($)
Fremont PD AXS Console Solution: (6) AXS Consoles, DSC8000, MC8000 CCGW, (8) APX Consolettes, with Equipment and System Integration Services and Training; Includes First Year Warranty	$1,023,771
Nebraska State Discount Equipment Only (Contract 111563 O4)*	-$158,858
Additional Timing Discount*	-$64,869
TOTAL SYSTEM	**$800,044**
* Note 1: For these system discounts to apply a signed purchase order provided under the terms and conditions stated in the Contract No. 111563 O4 signed between Motorola Solutions, Inc. and the State of Nebraska must be submitted by December 12th, 2025 for all items and services as proposed.	

8.2 Lifecycle Services

Essential Plus & Lifecycle Services	TOTAL Yrs. 2 - 6
Essential Plus & Lifecycle Services - Year 2	$75,468
Essential Plus & Lifecycle Services - Year 3	$78,110
Essential Plus & Lifecycle Services - Year 4	$80,857
Essential Plus & Lifecycle Services - Year 5	$83,715
Essential Plus & Lifecycle Services - Year 6	$86,687
POST WARRANTY SERVICES TOTAL:	**$404,837**

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.

Section 9

Payment Terms

Except for a payment that is due on the Effective Date, Customer will make payments to Motorola within forty five (45) 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. **60% of the Contract Price due upon shipment of equipment from Staging;**
3. **10% 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.

INFLATION REVIEW. For multi-year agreements, at the end of the first year of the Agreement 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%. "All Items," not seasonally adjusted shall be used as the measure of CPI for this price adjustment. The adjustment calculation will be based upon the CPI for the most recent twelve (12) month increment beginning from the most current month available as 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).

For Lifecycle Support Plan and Subscription Based Services:
Motorola will invoice Customer annually in advance of each year of the plan.

Section 10

Contractual Documentation

The products and services offered in this proposal shall be provided under the terms and conditions stated in the Contract No. 111563 O4 signed between Motorola Solutions, Inc. and the State of Nebraska.

In addition, Motorola is required and hereby agrees to use a federal immigration verification system to determine the work eligibility status of new employees physically performing services within the State of Nebraska. A federal immigration verification system means the electronic verification of the work authorization program authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. 1324a, known as the E-Verify Program, or an equivalent federal program designated by the United States Department of Homeland Security or other Federal agency authorized to verify the work eligibility status of a newly hired employee.