MOTOROLA SOLUTIONS

CITY OF HUDSON

MCC 7500 DISPATCH CONSOLE PROJECT **OCTOBER 31, 2019**

The design, technical, pricing, and other information (“Information”) furnished with this submission is proprietary and/or trade secret information of Motorola Solutions, Inc. (“Motorola Solutions”) and is submitted with the restriction that it is to be used for evaluation purposes only. To the fullest extent allowed by applicable law, the Information is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the Information without the express written permission of Motorola Solutions.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2019 Motorola Solutions, Inc. All rights reserved.

October 31, 2019

Sgt. Dan Thompson
36 S. Oviatt St.
Hudson, Ohio 44236

RE: Motorola Solutions Hudson, OH MCC7500 Proposal PS-000095835

Dear Mr. Thompson,

Motorola Solutions, Inc. (Motorola Solutions) appreciates the opportunity to provide City of Hudson with quality communications equipment and services. Motorola Solutions' project team has taken great care to propose a solution to address your needs and provide exceptional value.

To best meet the functional and operational specifications, our solutions include a combination of hardware, software, and services. Specifically, this solution provides (2) two MCC7500s and (1) one MCC7500E, as well as implementation and warranty services needed to support them.

This proposal is based on and subject to the terms and conditions of Ohio State Term Schedule Contract 573077 and shall remain valid for a period of 90 days from the date on this letter. The City may accept the proposal by delivering to Motorola a purchase order referencing Ohio STS 573077. Alternatively, Motorola would be pleased to address any concerns the City has regarding this proposal. Any questions can be directed to Hannah Lindesmith, Account Executive at 330-209-4051, (Hannah.lindesmith@motorolasolutions.com).

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

Sincerely,

Joe Tee
Account Sales Manager

MOTOROLA SOLUTIONS, INC.

TABLE OF CONTENTS

Section 6

Section 7

SECTION 1

SYSTEM DESCRIPTION

1.1 OVERVIEW

The City of Hudson Dispatch Center console technology enhancement project consists of:

1) **Motorola MCC 7500 dispatch console equipment**—This quotation is for a technology upgrade and replacement of the existing dispatch console positions with three new Motorola MCC 7500 IP-based operator position, and the addition of IP network hardware to support both trunking and conventional operations. For this proposal Motorola is providing two MCC 7500 positions with the associated Voice Processor Module in the main dispatch room and one MCC 7500E position to be located in the lower level for the dispatch center.

2) **Interoperability** - The implementation of this upgrade will ensure full interoperability with the Ohio MARCS*IP* trunked statewide radio network

3) **Conventional Resources/Consolettes** - Motorola will interface to existing ten conventional resources and four proposed new APX consolettes, into the IP-based MCC7500 console system.

4) **Master Site Licenses** – Motorola has included the Master Site licenses to be added to the MARCS Zone 2 master site in support of the equipment provided with this proposal.

The replacement and upgrade has been designed to modernize and improve functionality of the radio network and existing dispatch operations at City of Hudson Dispatch. This equipment upgrade utilizes the new technology of IP-based consoles and is compatible with requirements for operation on the Ohio MARCS*IP* trunked statewide radio network.

1.2 DISPATCH CONSOLE EQUIPMENT

The MCC 7500 consoles are Motorola's second generation IP architecture console subsystem and are supported by the same IP network and switching that manages the MARCS*IP* ASTRO 25 trunked network. The MCC 7500 console equipment connects directly to the trunking system's transport network, eliminating the traditional circuit-based infrastructure. It uses IP-based packet protocols for passing call control data and call audio through the system.

The MCC 7500 is a state-of-the-art console system that features an enhanced version of the intuitive, Graphical User Interface (GUI). It operates on the Microsoft Windows 10™ platform, and the screen layout is simple and uses valuable space efficiently. Key information and critical functions are clearly identified with easy to understand icons. Dispatchers can quickly recognize these icons instead of reading text which maximizes productivity.

1.2.1 Dispatch Console Overview

City of Hudson dispatch migration to MCC 7500 wireline consoles allows for full utilization of Ohio MARCS console integrated elements including:

- Console dispatcher outbound message priority.
- Console initiated Call Alert.
- Inter Zone Communications (statewide).
  - Talkgroup Call
  - Announcement Talkgroups
  - Call Alert
  - Multi-Group Call
- Console Patch
- Console Multi Select
- Integrated Dual Instant Recall Recorder (IRR)

The proposal includes three new operator position, two MCC 7500s and one MCC 7500E, at City of Hudson Dispatch, along with Conventional Site Controller (CSC), Enhanced Conventional Channel Gateway IP to analog interface units (ECCGW), and other networking equipment.

Included for each MCC 7500 operator position is a new computer workstation. The new HP Z2 Mini workstation will be equipped with Microsoft Windows 10 operating system, required for integration into the Ohio MARCS console network. The workstation will be provisioned with anti-virus software packages and intrusion resistant hardware to provide increased information security on the Ohio MARCS*IP* statewide radio network. The backup MCC 7500E position will used an HP ZBook equipped with Microsoft Windows 10 operating system.

Each proposed MCC 7500 dispatch position includes the following:

- HP Z2 Mini Workstation
- 22-inch LCD touch screen display.
- RF interference-free certified keyboard and mouse.
- A separate Voice Processing Module (VPM) for all other I/O connections.
- ADP Encryption.
- Dual Instant Recall Recorder with Z2 Mini Sound card and cables
- 4 desktop speakers (optionally expandable, up to eight).
- 2 headset jacks.
- A desktop microphone with built-in transmit button.
- A dual pedal footswitch to activate transmit and channel monitor functions.

The proposed MCC 7500E dispatch position includes the following:

- HP HP ZBook 15 G6
- Software License for up to 15 simultaneous calls
- Includes ADP encryption and also supports AES and DES Encryption
- Enhanced Instant Recall Recorder
- USB DVDE Drive
- Audio Interface Module
- Trackball pointing device
- 2 desktop speakers

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

- 2 headset jacks.
- A desktop microphone with built-in transmit button.
- A dual pedal footswitch to activate transmit and channel monitor functions.

The MCC 7500 console sub-system is tightly integrated into the ASTRO 25 digital voice system. The operator workstation will be linked with the zone master site for call audio, identification of calling radios including emergency alerts, and configuration of the display screens.

1.3 MCC 7500 VPM FEATURES AND BENEFITS

Designed for effective, flexible dispatch communications, the MCC 7500 VPM Dispatch Console provides a range of valuable features:

- Seamless integration with ASTRO® 25 trunking systems.
- IP Network—The MCC 7500 VPM supports the IP protocols of the ASTRO 25 system's transport network.
- End-to-End Encryption—Encryption and decryption occurs in the dispatch consoles, allowing true end-to-end encryption in the radio system.

Centralized System Management—The MCC 7500 VPM console system is configured and managed by the ASTRO 25 system's configuration manager, fault manager, and performance reporting applications. This provides Dispatch with a single point for configuring and managing the entire radio system, including the console portion. This information can also be accessed from multiple remote locations, providing Dispatch with convenient access while enjoying the benefits of centralized system management.

User-Friendly—MCC 7500 VPM's environment features the familiar standards used by other Windows programs worldwide.

Screen layout, menus and icons are easy to understand and quickly recognizable by users.

Easy dispatcher's display screen configuration can be customized via the Elite Admin application.

Elite Dispatch GUI uses a simple point-and-click response. The dispatcher has the choice of using a standard mouse or optional trackball, and the keyboard is not required for day-to-day dispatch operations. A mouse is offered with this proposed design.

Agency Partitioning—Allows multiple agencies to use a common system while maintaining control over their console resource.

1.3.1 Architecture

There are three main components of a Motorola MCC 7500 VPM system:

- Dispatch console.
- IP routing and site control equipment.
- Conventional Channel Gateway.

Various combinations of these components are connected together and to the rest of the ASTRO 25 system via a console site router and switch on an IP network.

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

The dispatch console software consists of the Elite Dispatch graphical user interface (GUI), explained in this system description. The dispatch console hardware is based on a commercially available personal computer with Motorola-provided hardware and software.

Available Motorola-certified personal computer accessories for each dispatcher position include (see equipment list for the proposed accessories):

- A display monitor.
- RF interference-free certified keyboard and mouse.
- A separate Voice Processing Module (VPM) for all other I/O connections.
- Desktop speakers (optionally expandable, up to eight).
- Dual IRR speakers.
- Headset jacks.
- A desktop microphone with built-in transmit button.
- A dual pedal footswitch to activate transmit and channel monitor functions.

The Voice Processor Module (VPM) includes the voice card which performs the digital-to-analog and analog-to-digital conversions for all analog audio flowing into or out of the dispatch console. It also provides the connections for accessory items including speakers, headset jacks, microphone, footswitch, telephone headset audio, and instant recall recorder for radio.

The VPM provides the vocoding and audio processing services for the dispatch console. It includes AMBE and IMBE vocoder algorithms for ASTRO 25 operation, as well as supporting audio level adjustments, summing and filtering, and can support multiple simultaneous streams of audio. The VPM also generates standard paging tone sequences used for personnel alerting.

1.3.2 Elite Dispatch Graphical User Interface

The Motorola MCC 7500 dispatch console uses the Elite Dispatch graphical user interface (GUI) for displaying information to and accepting commands from the dispatcher. The Elite Dispatch GUI is efficient, easy to use, and intuitive having been refined and proven through years of use in public safety dispatch centers around the world, including Ohio MARCS. The Elite GUI is periodically updated and enhanced to improve flexibility and versatility in public safety dispatch centers with from one to over one hundred operator positions.

An example of the Elite Dispatch GUI is shown below in Figure 1-1.

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

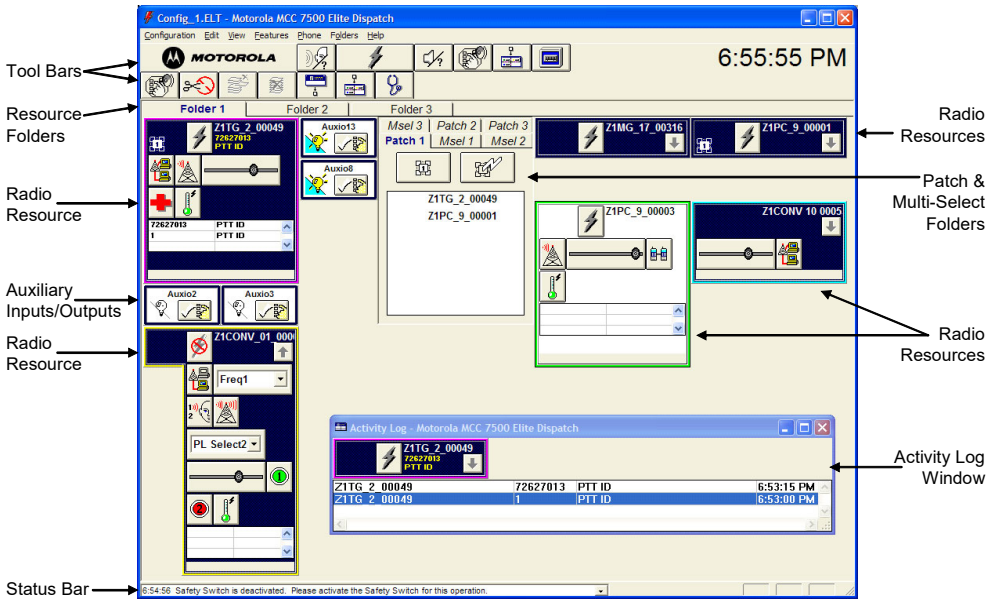

Figure 1-1: Elite Dispatch GUI

The Elite Dispatch GUI is based on Microsoft Windows GUI programming standards and contains many controls, displays and features which are familiar to anyone who has used Windows-based applications. These features are described in greater detail in the following sections.

1.3.2.1 Pull-Down Menus

The dispatcher is able to access features and functions through the pull-down menus. The Elite Dispatch GUI provides the following pull-down menus on a menu bar across the top of the dispatch window.

- **Configuration**—Provides access to the configuration files used by the Elite Dispatch GUI. Also allows the dispatch application to be exited.
- **Edit**—Allows various aspects of how audio, resources and features are presented to the user on the Elite Dispatch GUI to be edited. Changes made using this menu are not permanent and are lost when the dispatch application is exited.
- **View**—Allows the dispatcher to control whether or not the Activity Log and Auxiliary I/O Windows are shown.
- **Folders**—Allows the dispatcher to switch between folders, add folders and change the folder tab width. Changes made using this menu are not permanent and are lost when the dispatch application is exited.
- **Help**—Provides access to detailed online help for using the Elite Dispatch GUI.
- The user may customize which menus are displayed and what they contain via the Elite Admin application.

1.3.2.2 Toolbars

The toolbar is a row of icon buttons located at the top of the dispatch window. Up to two toolbars may be present and may be used to provide quick access to frequently used features. The following are examples of the items which may be placed in the toolbars:

- Clock.
- General transmit button.
- Alert tone selections.
- Monitor button.
- All mute button.

There are many other items which may optionally be placed in the toolbars. The Elite Admin application is used to define how many toolbars are displayed and what they contain.

1.3.2.3 Status Line

A status bar is provided across the bottom of the dispatch window for viewing the status of the dispatch console, as well as various error messages. The most current status or error message is displayed in the status line until cleared by the dispatcher. The dispatcher may scroll through the last ten statuses/error messages to view them and may clear them by using the Features menu on the menu bar.

1.3.2.4 Resource Folders

The Elite Dispatch GUI provides up to six resource folders for organizing the various resources (radio resources, one-button paging, auxiliary input/output resources, etc.) that are assigned to the dispatch console. These folders may be given descriptive names to simplify the organization of the resources.

The resources on a folder are displayed when the dispatcher clicks on the folder tab. Resources on folders which are hidden behind the one being displayed continue to operate in a normal manner. Radio resource audio on a hidden folder appears in the appropriate speakers/headsets along with a visual call indication on the folder tab. If an emergency alarm or call is received on a radio resource which is located on a hidden folder, a visual emergency indication is displayed on the folder tab.

A resource may be placed in more than one folder at the same time. This allows City of Hudson Dispatch to create folders for special situations without having to move resources back and forth between folders.

The Elite Admin application is used to configure how many folders appear on the Elite Dispatch GUI and which resources appear on each folder. It is also used to set the descriptive names which appear on the folder tabs.

During dispatch operations the dispatcher may, if so configured by the Elite Admin application, be able to temporarily add, remove or move resources on the folders. If this is done these changes are not saved when the user logs out of or changes configuration files for the dispatch application.

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

Radio Resources

Voice communication paths in the radio system are represented as radio resources—also referred to as tiles—on the Elite Dispatch GUI. These radio resources are used by the dispatcher to communicate on and control the radio system.

The following radio resources are supported:

- Trunked Talkgroups.
- Trunked announcement groups.
- Trunked private calls.
- Analog conventional channels.

Indicators and Controls

A radio resource contains indicators and controls that allow the dispatcher to monitor and control various aspects of the radio channel. Examples of the indicators and controls which may appear on a radio resource include:

- Instant transmit button.
- Transmit active/transmit busy indications.
- Patch active/patch busy indications.
- Received call indication.
- Received call stack.
- Individual volume control.

The types of indicators and controls which appear on the radio resource depend on the type of radio channel it represents, and how it has been configured in the Elite Admin application. The radio resource may be configured as a compressed resource, a larger compressed resource or an expanded resource.

- **Compressed Resource**—Allows the dispatcher to hide the indicators and controls the radio resource (Figure 1-2). The small arrow button opens and closes the resource to show the controls and indicators. This saves a tremendous amount of space on the screen by allowing the dispatcher to view only the most critical information for any given channel. This type of display is ideal for dispatchers monitoring several different channels where space in the resource folder is at a premium.

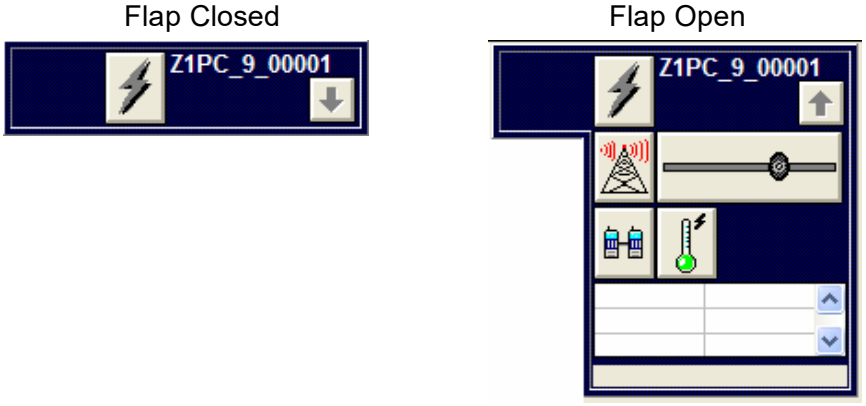

Figure 1-2: Compressed Radio Resource

- **Larger Compressed Resource**—A radio resource that always shows some of the indicators and controls, but allows the dispatch console to hide some of the others (Figure 1-3).

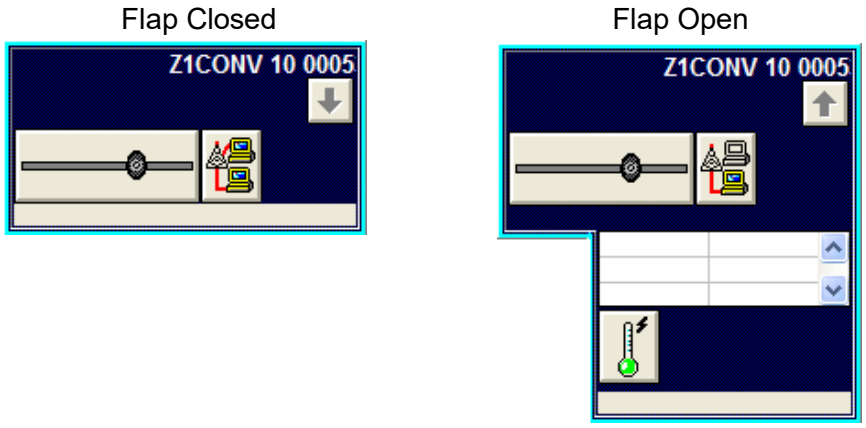

Figure 1-3: Larger Compressed Radio Resource

- **Expanded Resource**—This radio resource always shows the indicators and controls (Figure 1-4) and cannot be compressed. The expanded version provides the advantage of a single-button press for any function. It is ideal for dispatchers who are only monitoring a few channels/talk groups and where space in the resource folder is not at a premium.

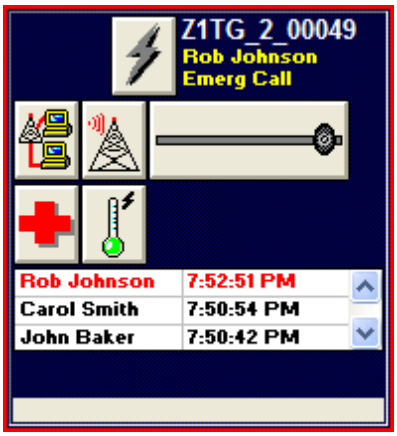

Figure 1-4: Expanded Radio Resource

Any activity or change on a radio resource appears on all dispatch consoles that have that resource assigned on them.

Received Call Stack

The received call stack provides the dispatcher with a visual record of the most recent inbound calls on radio resources. This allows the dispatcher to keep track of calls during busy traffic periods. The calls are displayed in list format on a radio resource, with the most recent calls at the top of the list. The number of calls displayed in the list is configurable, as is the type of information displayed. The types of information that can be displayed include: unit ID, unit ID alias, site ID, zone ID, type of call and time. If an alias is available for a piece of information, it is displayed; otherwise the raw information is displayed. Figure 1-5 shows a radio resource containing a received call stack.

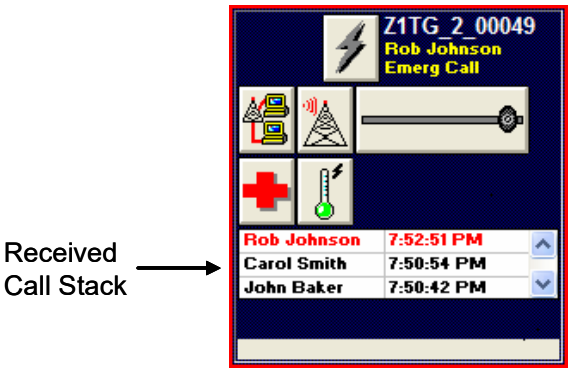

Figure 1-5: Received Call Stack on a Radio Resource

The received call stack has a fixed memory of 25 calls, but the number of calls which are displayed is configurable via the Elite Admin application. Regardless of how many calls are actually displayed, the dispatcher can always scroll through all 25 calls in the stack's memory.

The dispatcher can delete individual calls from the received call stack. All of the calls listed in a received call stack can also be deleted with a single action.

1.3.2.5 Auxiliary Input and Output Resources

Auxiliary inputs and outputs (Aux I/Os) allow control of external devices via relay closures and sense the state of external devices via input buffers from the MCC 7500 VPM Dispatch Console.

The Aux I/O resources are represented by various graphical icons that change their appearance based on the state of the resource. The Elite Admin application is used to associate a particular icon with a specific input or output. Examples of some of the icons which may be used are shown in Figure 1-6.

Icon for Input Buffer (shown in Active State)

Icon for Control Relay (shown in Active State)

Icon for Control Relay (shown in Inactive State)

Figure 1-6: Auxiliary Input/Output Resource Icons

1.3.2.6 Patch and Multi-Select Folders

The patch and multi-select features are accessed via a set of dedicated folders on the Elite Dispatch GUI. These folders are smaller than the resource folders, and may be placed on the screen to suit the dispatcher's preferences. The placement is done in the Elite Admin application. There can be up to 16 patch folders and three multi-select folders.

Patch Folders

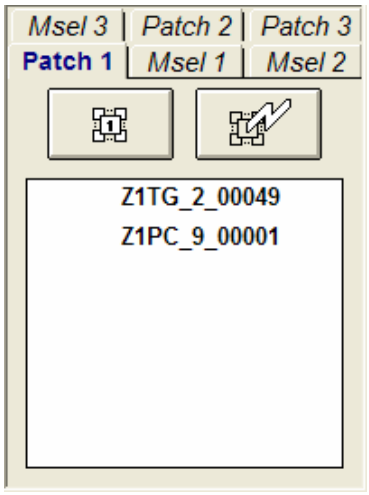

Figure 1-7: Patch Folders

Clicking on one of the patch folder tabs brings it into view. The patch group is then opened by clicking on the left-most button on the folder. Once the patch group is open, the patch group is editable and members may be added or removed from the patch group by clicking on the desired radio resources. Note that patch groups are active whenever there are members assigned to them. This is true even if the patch group is not open.

The members of the patch group are shown on the patch folder along with the status of each member (patched or pending). The resources in the patch also show an indication that they are in a patch group.

Some patch groups contain members which were pre-assigned by the Elite Admin application. These patch groups become active as soon as possible after the dispatch console begins using the configuration file which contains the pre-assigned patch groups. The dispatcher can add/remove members from the pre-assigned patch group, but these additions/removals are lost when the dispatch console either re-loads the configuration file or changes to a different configuration file.

A patch transmit button is provided on the patch folder to allow the dispatcher to easily transmit on all members of the patch group with a single button press.

Multi-Select Folder

Clicking on one of the multi-select folder tabs brings it into view. The multi-select group is then opened by clicking on the left-most button on the folder. Once the multi-select group is open, the multi-select becomes active, and members can be added or removed from the group by clicking on the desired radio resources. Closing the multi-select folder (by clicking on the left-most button a second time) deactivates the multi-select group.

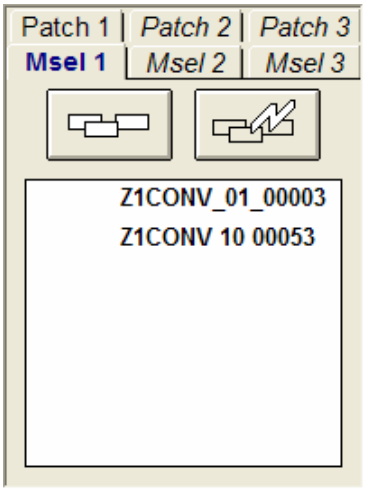

Figure 1-8: Multi-Select Folder

NOTE: This operation is different than that of the patch folders. A dispatch console can only have one multi-select group active at a time, but it can have multiple patch groups active simultaneously.

The members of the multi-select group are shown on the multi-select folder. Some multi-select groups contain members which were pre-assigned by the Elite Admin application. The dispatcher can add/remove members from the pre-assigned multi-select group, but these additions/removals are lost when the dispatch console either re-loads the configuration file or changes to a different configuration file.

1.3.2.7 Activity Log Window

The dispatcher can use the activity log window as a point of reference for all calls coming into the dispatch console. The activity log shows call information associated with all incoming radio calls including the name of the radio resource and the time of the call. Incoming calls from all radio resources assigned to the dispatch console are displayed in the activity log.

Figure 1-9 shows an example of an activity log window.

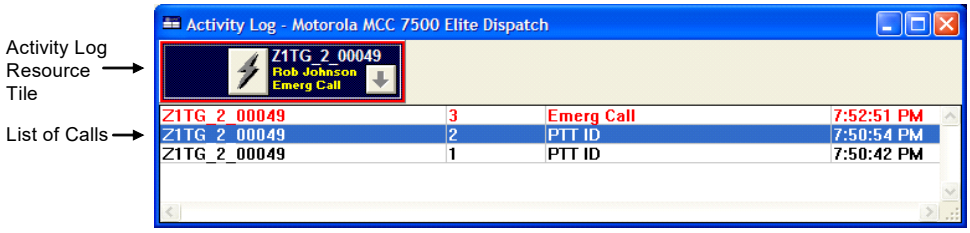

Figure 1-9: Activity Log Window

Up to 1000 calls can be held in the activity log. The most recent call is in top of the list and the oldest is at the bottom. Once the list is filled, the oldest calls are discarded as new calls come in. the dispatcher may resize the activity log to show various numbers of calls. For example, when there is light activity, the dispatcher may choose to only show a few calls. During busy hours, the dispatcher may view more calls by simply dragging the lower right hand corner of the activity log (making it longer) to see additional calls.

Dispatchers may respond to incoming calls by clicking on a call in the list. Once a call is selected, the entry appears highlighted and the name of the radio resource appears at the top of the activity log. The dispatcher can then press the instant transmit button on the activity log resource tile to communicate with that radio resource.

The information displayed by the activity log can be customized to suit the dispatcher's needs. The activity log can be configured to show combinations of Resource Name, Unit ID or Alias, Status Number or Alias, Receiving Site ID, Receiving Zone ID and Time. This configuration is done via the Elite Admin application and, if so configured, via the dispatcher interface.

The Elite Admin application controls whether or not a dispatch console has the capability of displaying the activity log. If a dispatch console is given the capability, the dispatcher has the ability to view or not view the activity log based on their needs.

The number of lines that are initially displayed by the activity log is configurable via the Elite Admin application or the dispatcher interface. The number of lines that are displayed may

also be changed in real-time by changing the size of the activity log window. The user can scroll through all the entries in the activity log, even if they cannot all be displayed at once.

1.3.2.8 Help

The dispatch console is designed to allow the dispatcher to quickly access information on how to use its features. There are three types of help available to the dispatcher: Online, Micro and Tool Tips.

Online Help

Online Help provides detailed information on how to use the dispatch console. The user accesses Online Help via the Help menu on the menu bar. The user can search for topics or key words to quickly find the desired information or the user can use a table of contents to find the information. The information is displayed in a pop-up window on the dispatch user interface.

Online Help allows new dispatchers to shorten their learning curve and more experienced dispatchers to quickly remember how to operate seldom-used features.

Micro Help

Micro Help provides information about the state of controls or indicators in a resource tile. When the cursor is placed over a control or indicator on a resource tile, a description of the control or indicator's state is given across the bottom of the resource tile. The text across the bottom of the resource describes the icon the cursor is pointing to.

The text displayed by the Micro Help feature may be edited via the Elite Admin application.

Micro Help allows a dispatcher to view the status of a control or indicator textually instead of graphically.

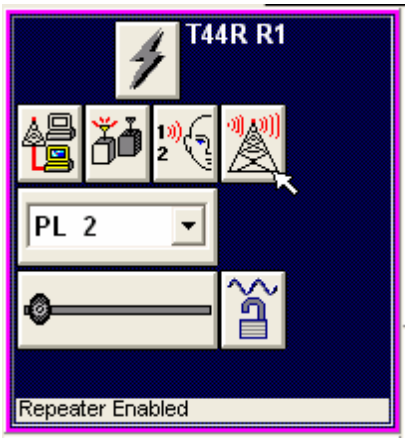

Figure 1-10: Micro Help on a Radio Resource

Tool Tips Help

Tool Tips Help provides information about tool bar buttons and menu bar menus to the dispatcher. When the cursor is placed over a tool bar button, the button's name appears in a small pop-up window next to the cursor, and a short explanation of the button appears in the status bar at the bottom of the dispatch user interface window. When the cursor is moved across a menu item in a menu, a description of the menu item appears in the status bar at the bottom of the dispatch user interface window.

The text displayed by the Tool Tips feature may be edited via the Elite Admin application. Tool Tips allow a dispatcher to quickly see a short explanation of the button or menu item of interest.

1.3.2.9 MCC 7500E Operator Position

The MCC 7500E Dispatch Console and the MCC 7500 Dispatch Console share a large number of feature and operational similarities. The conventional channel gateways (CCGWs), conventional site controllers (CSCs), Aux I/O Servers, and other items that are

associated with the dispatch position are the same as with the MCC 7500 dispatch positions and don't change when used with MCC 7500E dispatch positions. The MCC 7500E dispatch position offers scalable capacity and flexible deployment options and is a software-based dispatch console that requires no external hardware connections (no VPM) to perform dispatch operations. Audio Vocoding is performed within the Windows operating system. The main difference with the MCC 7500E position provided with this proposal is that it is software limited to 15 simultaneous audio sources.

1.3.3 Elite Admin Application

The Elite Dispatch GUI screens are configured using the Elite Admin application. This application is designed to be extremely flexible and powerful, and allows administrators to build display screens that look very simple with minimal icons and channels, or more sophisticated with many folders and channels. The Elite Admin application allows Ohio MARCS trained and authorized technical support staff to create screens that can be used by multiple dispatchers (accessed over the network), shared by all users of a single position, or even a customized screen per dispatcher. Each screen configuration may optionally be password protected to ensure proper use and control. All of the screen configurations could be stored on the state's servers.

The state's personnel use the Elite Admin application to perform numerous functions including:

- Create new configurations (for any operator).
- Enable or disable operator positions.
- Modify existing configurations.
- Assign/de-assign radio resources to various folders and determine location.
- Determine audio routing of resources to speakers.
- Set initial volume level of radio and phone resources.
- Determine icons used for AUX I/Os.
- Determine if Auxiliary I/Os are safety switch protected, and whether they have an audible alarm.
- Determine items that should go on the toolbar and where they should be placed.
- Create pre-assigned patch/multi-select/primary groups.
- Create pre-assigned one-button paging tone sequences.
- Determine if the activity log is shown initially and where on the screen it is shown (dispatchers may still hide or show the activity log).
- Assign/de-assign radio and auxiliary input/output resources to various folders.
- Determine where features are placed on each radio resource.
- Determine the size of each radio resource (compressed, larger compressed or expanded).

1.4 OHIO MARCS REDUNDANT CORE NETWORKING

The Ohio MARCS zone core equipment includes redundant Master site controllers, system routing centers, LAN switches, and other ancillary equipment.

The core includes AES data encryption on all IP links extending outside the core location, including dispatch centers and to CCGW devices located at remote base station sites. Link encryption is a general best practice for IP-based communications networks in the public

safety mission critical realm, and is required for interconnection with Ohio MARCS statewide communications infrastructure. The core link encryption capability does not provide protection for analog telephone line connections between the CCGW ports and individual base or control stations.

All entities connecting to OH MARCS*IP* Trunking system enjoy the benefits of highly robust environment and higher security standards as described above.

1.5 CONVENTIONAL CHANNEL GATEWAYS

The Conventional Channel Gateway (CCGW) is part of the core networking equipment used with the MCC 7500 VPM Dispatch Console to provide the dispatchers access to analog conventional stations that are terminated at the City of Hudson Dispatch center. These will also include the four new APX 7500 Consolette control stations supplied with this proposal. The CCGW allows an analog conventional base station, audio source, or digital channel to connect to the IP transport network and the console system. When the base stations with gateways are connected to the network, dispatchers are able to monitor and transmit on the radio channel.

City of Hudson Dispatchers will have communications capability on analog conventional radio channels in addition that are local to the dispatch center and also to the Ohio MARCS digital P25 trunked radio network. Existing control stations and other conventional RF resources will be connected into the IP network via Conventional Channel GateWay (CCGW) units which translate between the analog audio control information and IP data packets.

Each conventional base station radio and interoperability channels will have an IP interface converter connection so they can be accessed by the new MCC 7500 IP-based consoles. The proposed system includes three CCGW units and redundant site routers. Each ECCGW supports up to eight control interfaces, two-wire and four-wire interfaces are supported interchangeably.

The system provides Audio Logging Output. A method to play back audio/view logged information is provided by the existing *third-party solution*. The Voice Processing Module (VPM) utilizes the following ports: External Paging Encoder Port, Telephone/Headset Port, Instant Recall Recorder Port, and Long Term Logging Port. The Long Term Logging Port allows an *external logging recorder* to be connected to an MCC 7500 Dispatch Console. The audio that appears on this output is *selected speaker*. Typically, it is the audio that was transmitted and/or received at that MCC 7500 Dispatch Console.

Motorola Logging solution, based on the service available from MARCS, is *NOT included* in this proposal by customer's request.

1.6 CONSOLETTES

The Motorola APX™ 7500 Consolette is the next generation Consolette design that incorporates the APX 7500 mobile transceiver and the O5 control head.

City of Hudson Dispatch Center requested 800/700 MHz consolettes only. Proposed configurations include the full front panel consolette option. Rear panel interfaces include:

Tone Remote Control (TRC), ACIM, and E&M (Ear and Mouth) for interfacing to remote consoles and desksets such as the MCC 7500.

All models are equipped with an internal AC-to-DC power supply and support Battery Revert operation. In addition to the above mentioned functionality, the APX 7500 Consolette supports the following functionality via its rear panel: recorder interface, connection for up to two headsets, interface for connection of an external PA, connection for a second speaker, and a crosspatch interface.

1.7 CONSOLE ALIAS MANAGER

The MKM 7000 Console Alias Manager (CAM) software is a solution for creating, editing and distributing the Radio Unit ID Aliases used on the MCC 7500 IP dispatch consoles.

It was developed in response to customer requests for greater flexibility and more capabilities in managing these aliases. Console Alias Manager provides the following primary benefits:

- Autonomy in managing aliases.
- Faster distribution of updated aliases to consoles.
- An API for connecting to CAD or other systems.

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

SECTION 2

EQUIPMENT LIST

QTY	NOMENCLATURE	DESCRIPTION
1	SQM01SUM0273	MASTER SITE CONFIGURATION
1	CA02629AC	ADD: EXPAND 7.17 M CORE
1	UA00156AA	ADD: MCC7500 CONSOLE LICENSES (QTY 5)
1	CA01316AA	ADD: UNC ADDTL DEVICE LIC (QTY 10)
1	B1905	MCC 7500 ASTRO 25 SOFTWARE
2	B1933	MOTOROLA VOICE PROCESSOR MODULE
2	CA01642AA	ADD: MCC 7500 BASIC CONSOLE FUNCTIONALITY SOFTWARE LICENSE
2	CA01643AA	ADD: MCC 7500 / MCC 7100 TRUNKING OPERATION
2	CA00147AF	ADD: MCC 7500 SECURE OPERATION
2	CA00245AA	ADD: ADP ALGORITHM
2	CA00140AA	ADD: AC LINE CORD, NORTH AMERICAN
2	DSEV221B	TECH GLOBAL EVOLUTION SERIES 22INCH WITH TOUCH
2	TT3492	Z2 G4 MINI WORKSTATION NON RETURNAB
2	T7448	WINDOWS SUPPLEMENTAL FULL CONFIG
8	B1912	MCC SERIES DESKTOP SPEAKER
2	B1914	MCC SERIES DESKTOP GOOSENECK MICROPHONE
4	B1913	MCC SERIES HEADSET JACK
4	RLN6099A	HDST MODULE BASE W/PTT, 25 FT CBL
6	RMN5150A	OVER-THE-HEAD, MONAURAL, NOISE-CANCELING HEADSET
2	DSTWIN6328A	PROVIDES ONE DUAL PEDAL FOOTSWITCH FOR USE WITH MOTOROLA MCC 7500 DISP
3	T7885	MCAFEE WINDOWS AV CLIENT
2	DDN2089	DUAL IRR SW USB HASP WITH LICENSE (V47)
2	DSICUSBAUDIO7D	STARTECH 7.1 USB AUDIO ADAPTER SOUND CARD
2	DDN9649	INSTANT RECALL RECORDER CABLE FOR MCC 7500
2	DSLOGITECHZ130	LOGITECH Z130 SPEAKERS
1	B1949	MCC 7500E SOFTWARE DVD
1	B1948	MCC 7500E DISPATCH POSITION LICENSES
1	UA00249AA	ADD: 15 RADIO RESOURCES LICENSE
1	UA00653AA	ADD: BASIC CONSOLE OPERATION
1	UA00654AA	ADD: ASTRO 25 TRUNKING OPERATION
1	UA00655AA	ADD: ADVANCED CONVENTIONAL OPERATION
1	UA00658AA	ADD: SECURE OPERATION

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

QTY	NOMENCLATURE	DESCRIPTION
1	UA00659AA	ADD: ADP/AES/DES-OFB ENCRYPTION
1	UA00661AA	ADD: ENHANCED IRR
1	DS8FQ02UTABA	ZBOOK 15 G6 I7-9850H 15 16GB/512 PC INTEL I7-9850H
1	DSF2B56AA	USB EXTERNAL DVD DRIVE
1	DSST7300U3M	STARTECH 7 PORT USB 3.0 HUB
1	DSCDN6171B	TRACKERBALL (ONLY PS/2 & USB COMPATIBLE)
1	B1941	USB AUDIO INTERFACE MODULE
2	B1913	MCC SERIES HEADSET JACK
1	B1914	MCC SERIES DESKTOP GOOSENECK MICROPHONE
2	RLN6099A	HDST MODULE BASE W/PTT, 25 FT CBL
1	DSTWIN6328A	PROVIDES ONE DUAL PEDAL FOOTSWITCH FOR USE WITH MOTOROLA MCC 7500 DISP
2	CDN6673	PC DESKTOP SPEAKERS
2	CLN1856	2620-24 ETHERNET SWITCH
4	CLN8490A	FRU: MINI GBIC (J4858B)
2	CKN6906A	FRU: FIBER CABLE
2	SQM01SUM0205	GGM 8000 GATEWAY
2	CA01616AA	ADD: AC POWER
2	CA02087AA	ADD: ENCRYPTION (7.12 OR LATER)
2	CA02108AA	ADD: DIRECT SHIP (NO STAGING)
1	F4543	SITE MANAGER BASIC
1	VA00874	ADD: AUX I-O SERV FW CURR ASTRO REL
3	V592	AAD TERM BLCK & CONN WI
1	T7038	GCP 8000 SITE CONTROLLER
1	CA00303AA	ADD: QTY (1) SITE CONTROLLER
1	X153AW	ADD: RACK MOUNT HARDWARE
1	CA01136AA	MCC 7500 CONVEN SITE OPER
1	CA00717AA	ADD: ASTRO SYSTEM RELEASE 7.17
1	SQM01SUM0205	GGM 8000 GATEWAY
1	CA01616AA	ADD: AC POWER
1	CA02087AA	ADD: ENCRYPTION (7.12 OR LATER)
1	CA02086AA	ADD: HIGH DENSITY ENH CONV GATEWAY
1	SQM01SUM0205	GGM 8000 GATEWAY
1	CA01616AA	ADD: AC POWER
1	CA02087AA	ADD: ENCRYPTION (7.12 OR LATER)
1	CA02086AA	ADD: HIGH DENSITY ENH CONV GATEWAY
1	SQM01SUM0205	GGM 8000 GATEWAY
1	CA01616AA	ADD: AC POWER
1	CA02087AA	ADD: ENCRYPTION (7.12 OR LATER)

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

QTY	NOMENCLATURE	DESCRIPTION
1	CA02086AA	ADD: HIGH DENSITY ENH CONV GATEWAY
1	TRN7343	SEVEN AND A HALF FOOT RACK
2	DSTSJADP	RACK MOUNT GROUND BAR, 19 IN FOR TSJ AND WPH SERIES DATA SPDS
1	DS11011173	PDU, AC EDGE RACK MOUNT DISTRIBUTION PANEL, 220-240VAC 60A
12	DS3750297	BREAKER, 15 AMP, CB UL 489 LISTED FOR AC EDGE II (1101-1188)
1	BVN1013	MKM 7000 Console Alias Manager Software
4	L30URS9PW1 N	APX CONSOLETTE 7/800
4	W969	ADD: MULTIPLE KEY ENCRYPTION OPERATION
4	G851	ADD: AES/DES-XL/DES-OFB ENCRYPTION
4	G90	ADD: NO MICROPHONE NEEDED
4	G806	ADD: ASTRO DIGITAL CAI OPERATION
4	G51	ENH: SMARTZONE OPERATION APX
4	G361	ENH: P25 TRUNKING SOFTWARE APX
4	CA01598	ADD: AC LINE CORD US
4	L999	ADD: FULL FP W/05/KEYPAD/CLOCK/VU
4	G78	ADD: 3Y ESSENTIAL SERVICE
4	HKN6233C	APX CONSOLETTE RACK MOUNT KIT
1	DSPCD013V8	8 CHANNEL COMBINER KIT, STANDARD ISOLATION, 851-870 MHZ
1	B1912	MCC SERIES DESKTOP SPEAKER
1	B1914	MCC SERIES DESKTOP GOOSENECK MICROPHONE
1	B1913	MCC SERIES HEADSET JACK
1	TT3492	Z2 G4 MINI WORKSTATION NON RETURNAB
1	B1934	MCC 7500 VOICE PROCESSOR MODULE FRU
1	CA00147AF	ADD: MCC 7500 SECURE OPERATION
1	CA00245AA	ADD: ADP ALGORITHM
1	CLN1856	2620-24 ETHERNET SWITCH
1	DLN6781	FRU: POWER SUPPLY

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

SECTION 3

STATEMENT OF WORK

3.1 OVERVIEW

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

The proposed system connects to the Ohio MARCS*IP* system.

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

3.1.1 Motorola's Responsibilities

Motorola's general responsibilities include the following:

- Conduct project kickoff meeting with the City of Hudson to review project design and finalize requirements.
- Schedule the implementation schedule in agreement with the City. Coordinate the activities of all Motorola subcontractors under this contract.
- Provide the City with the appropriate system interconnect specifications.
- Define link specifications for each link required for the proposed system.
- Define electrical requirements for each equipment rack and operator position to be installed in the City of Hudson-provided facilities.
- Define heat load for each equipment rack to be installed in the City of Hudson-supplied facilities.
- Administer safe work procedures for installation.
- Install the proposed console operator positions in the locations (1st floor and basement) and on desktop space provided by the City of Hudson.
- Install and configure the MKM 7000 alias manager.
- Include networking equipment (routers, switches) as needed at the main dispatch to interface to the MARCSIP system.
- Connect the console to the existing City of Hudson-provided circuits.
- Install a dedicated Local Area Network (LAN) at the dispatch center to connect the proposed console positions.
- Connect existing pre-wired auxiliary input/outputs (up to 5) to the Motorola SDM 3000 input/output box, as needed. NOTE: If additional inputs/outputs are needed this can be quoted separately.
- Install one (1) rack of dispatch backroom equipment within 100' of the console operator positions.
- Back room rack of equipment includes (see equipment list for additional detail):
  - Site Manager—Aux I/O SDM3000 with punchblock panel.
  - HP Ethernet switch.

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

  - Conventional Channel Gateway.
  - GCP 8000 site controller
  - Power Distribution Unit.
- Connect the appropriate equipment to City of Hudson-supplied ground system in accordance with Motorola's R56 Site Installation Standards.
- Perform the console programming, based on the console templates designed during the fleetmapping process jointly by Motorola and the City.
- Provide removal of existing customer owned console equipment after cutover is complete.
- Deliver removed console equipment to City of Hudson designated location.
- Connect the City of Hudson-supplied, previously identified circuits into the console, to a demarcation point located within 25 feet of the console interface.
- Interface existing 10 control stations/conventional resources (point of demarcation is the existing backroom).

NOTE: DC control is not supported. For any existing DC controlled resources these will need to be separately converted to Tone control. This conversion can be quoted if desired, otherwise, this is assumed to be City of Hudson responsibility.

- Install and configure the proposed 4, new, 700/800 MHz consolettes and combiner utilizing the existing customer provided antenna/line.
- Motorola is not responsible for interference caused or received by the Motorola-provided equipment except for interference that is directly caused by the Motorola-provided transmitter(s) to the Motorola-provided receiver(s). Should City of Hudson's system experience interference, Motorola can be contracted to investigate the source and recommend solutions to mitigate the issue.
- Integration of other third party products, not defined in this statement of work, is not included in this proposal.
- Perform R56 site installation quality audits, verifying proper physical installation and operational configurations at the City of Hudson dispatch location.
- Create site evaluation report to verify site meets or exceeds requirements, as defined in Motorola's "Standards and Guidelines for Communication Sites" (R56).
- Ohio MARCS Master site:
  - Provide infrastructure related programming of the proposed dispatch console site and operator positions into the Master site (i.e. add the new dispatch location, add consoles, loading of IDs into the zone controller).
- Optimize equipment and verify that all equipment is operating properly and that all electrical and signal levels are set accurately.
- Verify communication interfaces between devices for proper operation.
- Test features and functionality are in accordance with manufacturers' specifications.
- Verify the operational functionality and features of the dispatch subsystems and the system supplied by Motorola, as contracted.
- If any major task as contractually described fails, repeat that particular task after Motorola determines that corrective action has been taken.
- Document all issues that arise during the acceptance tests.
- Document the results of the acceptance tests and present to City of Hudson for review.
- Resolve any punchlist items before Final System Acceptance.

NOTE: Logging equipment and services are not included in this proposal. If desired, this can be quoted separately.

3.1.2 City of Hudson Responsibilities

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

- City of Hudson will provide a dedicated delivery point for receipt, inventory, and storage of equipment prior to installation.
- Coordinate the activities of all City of Hudson vendors or other contractors, if applicable.
- Attend and participate in project meetings and reviews.
- Provide ongoing communication, as applicable, with Ohio MARCS regarding the dispatch console project and schedule.
- Provide dispatch facility and antenna mounting locations as required for dispatch sub-system installation.
- Provide existing, installed/programmed control stations/consolettes (up to 10) with existing antenna and line and cabling to the backroom which can interface to the Motorola gateway in the backroom equipment rack.
- Ensure communications sites meet space, grounding, power, and connectivity requirements for the installation of all equipment.
- Obtain all licensing, site access, or permitting required for project implementation.
- Secure site lease/ownership, zoning, permits, regulatory approvals, easements, power, and Telco connections.
- Provide third party products and interface if needed.
- Provide demarcation point located within 25 feet of the console interface.
- Provide electrician for any electrical work required for R56 compliance and for installation, as needed.
- Provide clear and stable access to the sites for transporting electronics and other materials. Sufficient site access must be available for trucks to deliver materials under their own power and for personnel to move materials to the facility without assistance from special equipment.
- Supply adequately sized electrical service, backup power (UPS, generator, batteries, etc.) including the installation of conduit, circuit breakers, outlets, etc., at each equipment location. Provide AC power (dedicated 20 Amp AC outlets—simplex with ground) for each major piece of equipment within six (6) feet of the location of the Motorola-supplied equipment, including the associated electrical service and wiring (conduit, circuit breakers, etc.).
- Provide adequate HVAC, grounding, lighting, cable routing, and surge protection (also, among existing and Motorola-provided equipment) based upon Motorola's "Standards and Guidelines for Communication Sites" (R56). Ceiling [minimum nine (9) feet] and cable tray heights [minimum eight (8) feet] in the equipment rooms in order to accommodate seven (7)-foot, six (6)-inch equipment racks.
- Bring grounding system up to Motorola's "Standards and Guidelines for Communication Sites" (R56) and supply a single point system ground, of five (5) ohms or less, to be used on all FNE supplied under the Contract. Supply grounding tie point within 10 feet from the Motorola-supplied equipment.
- Provide floor space and desk space (including desk furniture, as needed) for the system equipment at the City of Hudson-provided facilities. Each rack shall be provided a minimum of
  24-inch x 24-inch footprint with 36 inches clearance in the front and back.

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

- Relocate and/or removal of existing equipment, if needed, to provide required space for the installation of Motorola-supplied equipment.
- Provide obstruction-free area for the cable run between the demarcation point and the communications equipment, as well as between the backroom equipment room and dispatch positions.
- Supply interior building cable trays, raceways, conduits, and wire supports.
- Resolve any environmental issues including, but not limited to, asbestos, structural integrity of the site, and any other building risks (resolve environmental or hazardous material issues).
- Provide console template and alias information as required for programming.
- Pay for usage costs of power and generator fueling, both during the construction and installation effort, and on an ongoing basis.
- Any required system network link resources will be provided by City of Hudson, per Motorola specifications for consoles to connect to the designated Ohio MARCS master site.
- Provide connectivity test results to confirm specification compliancy prior to equipment installation.
- Provide space for console cutover.
- Provide designated location for existing console equipment to be stored after removal.

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

SECTION 4

PROJECT SCHEDULE

Motorola's preliminary schedule indicates total project implementation to be approximately 4-6 months. This preliminary schedule is included for informational purposes only and assumes that all City of Hudson responsibilities as defined above are completed, as required. If site improvements or site approvals are needed these must be completed prior to equipment shipping to the field.

SECTION 5

TRAINING

5.1 PROPOSED TRAINING OVERVIEW FOR THE CITY OF HUDSON

In order to achieve the training goals identified by the City, we propose the following courses.

It is necessary that participants bring their laptop computers for all system administrator and technician classes. Materials will be delivered electronically via USB drives.

5.1.1 Console Operator and Supervisor Training Plan

Course Title	Target Audience	Sessions	Duration	Location	Date	Participants
MCC7500 Console Operator and Admin Utilizing the Interactive End User Tool Kit 3 training consoles (Instructor-led)	Dispatch Supervisors	1 (8-hour session)	1 day	US	Prior to cutover	3
MCC7500 Console Operator 3 training consoles (Instructor-led)	Dispatch Operators	2 (4-hour sessions)	1 day	US	Prior to cutover	12 (6 per session)

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

5.1.2 Course Descriptions for the City of Hudson

Course descriptions for the City are included on the following pages.

5.1.2.1 MCC 7500/MCC 7500E Console Supervisor

Course Synopsis and Objectives:	This course provides participants with the knowledge and skills to manage and utilize the MCC7500 console administrator functions. Through facilitation and hands-on activities, the participant learns how to customize the console screens. After completing this training course, you will be able to: - Understand the menu items and tool bar icons. - Edit folders, multi-select/patch groups, auxiliary input output groups, windows and toolbars. - Add/delete folders.
Delivery Method:	ILT - Instructor-led training
Duration:	4 hours Operator, plus 4 hours Admin
Participants:	Dispatch Supervisors and System Administrators
Class Size:	Based on number of Training Consoles available (2 students per Console)
Prerequisite:	None
Curriculum:	- Introduction. - Configurations. - Folders and Resource Setup. - Customizing Folders. - Auto Starting the MCC 7500 Dispatch Console. - Editing Preferences. - Configuring the Toolbar. - Setting Up Aux IOs. - Resource Groups.

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

5.1.2.2 MCC 7500/MCC 7500E Console Operator

Course Synopsis and Objectives:	This course provides participants with an introduction to the dispatch console, its basic operation and tailored job aids which will be available for assistance in operation. Through facilitation and hands-on activities, the user learns how to perform common tasks associated with the console operation. After completing this training course, you will be able to: - Perform basic operational tasks of the dispatch console. - Utilize the provided job aids to perform specific tasks associated with the console. - Understand a high level view of the system configuration. - Understand a high-level overview of the customer system configuration. - Understand general console operation. - Understand proper operating procedures for specific customer features.
Delivery Method:	ILT - Instructor-led training
Duration:	4 hours
Participants:	Dispatch Console Operators, Supervisors, System Administrators, and Support Personnel
Class Size:	Based on number of Training Consoles available (2 students per Console)
Prerequisite:	None
Curriculum:	- Overview. - Communicating with Radios. - Advanced Signaling Features. - Resource Groups. - Working with Configurations. - Working with Aux IOs. - Troubleshooting.

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

SECTION 6

WARRANTY/MAINTENANCE

Motorola places great emphasis on ensuring that communications systems, such as the one proposed for City of Hudson, meet high standards for design, manufacture, and performance. To enhance the value of the communications system being acquired, Motorola offers customized warranty.

6.1 WARRANTY SERVICES

Motorola Standard Commercial Warranty services are provided. In addition to the following services are also included in year 1 for the Motorola proposed new equipment.

NOTE: Lifecycle Services proposed are optionally available for maintenance and system upgrades after year 1. These services can be purchased with this proposal or as a separate purchase. As an Add On to Ohio MARCSIP all add-ons are required to align with the regular MARCSIP System Upgrade schedule through 2039 and must include security monitoring and security update services. See out years pricing in the Pricing Section.

6.2 ADVANCE PLUS SERVICES OVERVIEW

In order to ensure the continuity of City of Hudson's network and reduce system downtime Motorola Solutions proposes our Advanced Plus Services offering to the City. Appropriate for customers who wish to leverage Motorola Solutions' experienced personnel to maintain mission-critical communications for their first responders, Advanced Plus Services focuses on monitoring the network on an ongoing basis, proactively mitigating potential functionality and security issues, and providing both remote and on-site support. The proposed offering consists of the following specific services:

- Service Desk.
- Technical Support.
- Network Event Monitoring.
- On-site Support.
- Annual Preventative Maintenance.
- Network Hardware Repair with Advanced Replacement.
- Remote Security Patch Installation.
- Security Monitoring.
- Network Updates.

These services will be delivered to the City through the combination of local service personnel either dedicated to the network or engaged as needed; a centralized team within our Solutions Support Center (SSC), which operates on a 24 x 7 x 365 basis; and our Repair Depot, which will ensure that equipment is repaired to the highest quality standards. The collaboration between these service resources, all of who are experienced in the maintenance of mission-critical networks, will enable a swift analysis of any network issues, an accurate diagnosis of root causes, and a timely resolution and return to normal network operation.

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

6.3 ADVANCED PLUS SERVICES DESCRIPTIONS

6.3.1 Centralized Service Delivery

Centralized support will be provided by Motorola Solutions' support staff, located at our Service Desk and Solutions Support Center (SSC). These experienced personnel will provide direct service and technical support through a combination of Service Desk telephone support, technical consultation and troubleshooting through the SSC, and ongoing network monitoring of the City of Hudson's system.

Motorola Solutions will provide Service Desk response as a single point of contact for all support issues, including communications between the City, third-party subcontractors and manufacturers, and Motorola Solutions. When the City of Hudson's personnel call for support, the Service Desk will record, track, and update all Service Requests, Change Requests, Dispatch Requests, and Service Incidents using our Customer Relationship Management (CRM) system. The Service Desk is responsible for documenting the City of Hudson's inquiries, requests, concerns, and related tickets; tracking and resolving issues; and ensuring timely communications with all stakeholders based on the nature of the incident.

As tickets are opened by the Service Desk, issues that require specific technical expertise and support will be routed to our Solutions Support Center (SSC) system technologists for Technical Support, who will provide telephone consultation and troubleshooting capabilities to diagnose and resolve infrastructure performance and operational issues. Motorola Solutions' recording, escalating, and reporting process applies ISO 90001 and TL 9000-certified standards to the Technical Support calls from our contracted customers, reflecting our focus on maintaining mission-critical communications for the users of our systems.

The same SSC staff that provide direct telephone support to the City will also provide Network Event Monitoring to the City of Hudson's network in real-time, ensuring continuous management of the system's operational functionality. The SSC's technicians will utilize sophisticated tools to remotely monitor the City of Hudson's system, often identifying and resolving anomalous events before they might affect user communications.

6.3.2 Field Service Delivery

On-site repairs and network preventative maintenance will be provided by authorized local field services delivery personnel, who will be dispatched from and managed by the Solutions Support Center.

On-Site Support provides local, trained and qualified technicians who will arrive at the City of Hudson's location upon a dispatch service call to diagnose and restore the communications network. This involves running diagnostics on the hardware or Field Replacement Unit (FRU) in order to identify defective elements, and replacing those elements with functioning ones. The system technician will respond to the the City of Hudson'slocation in order to remedy equipment issues based on the impact of the issue to overall system function.

Annual Preventive Maintenance Service provides proactive, regularly scheduled operational testing and alignment of infrastructure and network components to ensure that they continually meet original manufacturer specifications. Certified field technicians perform

hands-on examination and diagnostics of network equipment on a routine and prescribed basis.

6.3.3 Network Hardware Repair

Motorola Solutions' authorized Repair Depot will repair the equipment provided by Motorola Solutions, as well as select third-party infrastructure equipment supplied as part of the proposed solution. The Repair Depot will manage the logistics of equipment repair (including shipment and return of repaired equipment), repair Motorola Solutions equipment, and coordinate the repair of third-party solution components.

Motorola Solutions also proposes **Network Hardware Repair with Advanced Replacement** to the City. With this additional service, Motorola Solutions will exchange malfunctioning components and equipment with advanced replacement units or Field Replacement Units (FRUs) as they are available in the Repair Depot's inventory. Malfunctioning equipment will be evaluated and repaired by the infrastructure repair depot and returned to the Repair Depot's FRU inventory upon repair completion. If the City prefers to maintain their existing FRU inventory, the City will be able to request a "loaner" FRU while their unit is being repaired.

6.3.4 Security Management Operations

The proposed **Remote Security Patch Installation Service** will provide the City with pre-tested security updates, pre-tested and remotely installed by Motorola Solutions on the City of Hudson's system. When appropriate, Motorola Solutions will make these updates available to outside vendors in order to enable them to test each patch, and will incorporate the results of those third-party tests into the updates before installation on the City of Hudson's network. Once an update is fully tested and ready for deployment in the City of Hudson's system, Motorola Solutions will remotely install it onto the City of Hudson's system, and notify the City that the patch has been successfully installed. If there are any recommended configuration changes, warnings, or workarounds, Motorola Solutions will provide detailed documentation along with the updates on the website.

Security Monitoring provides 24x7x365 monitoring of the radio network's security elements by specialized security technologists with years of experience working with ASTRO 25 mission-critical networks. For highly complex or unusual security events, our technologists have direct and immediate access to Motorola Solutions engineers for rapid resolution.

6.3.5 Network Updates

With our proposed **Network Updates Service**, Motorola Solutions commits to sustain the City of Hudson's ASTRO 25 system through a program of software and hardware updates aligned with the ASTRO 25 platform lifecycle. This comprehensive approach to technology sustainment will ensure that the City has access to the latest available standard features, as well as the opportunity to incorporate optional features through the purchase of hardware and/or software licenses. Updates and expansion of system components will optimize the availability of repair services, and will enable the City to add RF sites, dispatch positions, data subsystems, network management positions, and other elements to increase capacity and processing capability. Motorola Solutions will minimize any interruption to system operation during each network update, with minimal reliance on the City of Hudson's personnel.

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

6.4 MOTOROLA SOLUTIONS' SERVICES CAPABILITIES

Our focus on the needs of our public safety partners has led us to recognize that an integrated implementation and service delivery team that takes a new system from system installation, to acceptance, to warranty, and all the way through extended maintenance, is the best way to ensure that public safety communications systems meet the needs of first responders. Motorola Solutions' team of experts, have developed refined processes and sophisticated tools through our experience in delivering mission-critical communications.

6.4.1 On-Call Support through the Solutions Support Center (SSC)

The cornerstone of our customer care process, our Solution Support Center (SSC) is staffed 24x7x365 by experienced system technologists. This TL 9000/ISO 9001-certified center responds to over 5000 public safety, utility, and enterprise customers. With over 100,000 phone and email interactions with Motorola Solutions customers per month, the SSC provides our customers with a centralized contact point for service requests.

6.4.2 On-Site Service through a Field Service Team

On-site maintenance and repair of the City of Hudson's system will be provided by Motorola Solutions' local team of service personnel. Motorola Solutions will provide the City with a Customer Support Plan (CSP) that outlines the details of each service, provides escalation paths for special issues, and any other information specific to the City of Hudson's service agreement. Some of these details will include items such as access to sites, response time requirements, severity level definitions, and parts department access information.

Local technicians will be dispatched for on-site service by the SSC, who will inform the technician of the reason for dispatch. This will enable the technician to determine if a certain component or Field Replacement Unit (FRU) will be needed from inventory to restore the system. Once on site, the field technician will notify the SSC and begin to work on the issue. The technician will review the case notes to determine the status of the issue, and begin the troubleshooting and restoration process. Once the system is restored to normal operation, the field technician will notify the SSC that the system is restored. The SSC, in turn, will notify the City that the system is restored to normal operation and request approval to close the case.

6.4.3 Centralized Repair Management through Motorola Solutions' Repair Depot

Our repair management depot coordinates component repair through a central location, eliminating the need to send system equipment to multiple vendor locations for repair. Once equipment is at the depot, technicians will replicate the City of Hudson's network configuration in our comprehensive test labs in order to reproduce and analyze the issue. Technicians will then restore the equipment to working order. After repairs are completed, equipment will be tested to its original performance specifications and, if appropriate, configured for return to use in the City of Hudson's system. All components being repaired are tracked throughout the process, from shipment by the City to return through a case management system where users can view the repair status of the equipment via a web portal.

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

6.4.4 Direct Access to System Information through MyView Portal

Supplementing Motorola Solutions' proposed services plan for the City is access to MyView Portal, the Motorola Solutions' online system information tool (see the figure titled "MyView Portal"). MyView Portal provides our customers with real-time visibility to critical system and services information, all through an easy-to-use, graphical interface. With just a few clicks, the City of Hudson's administrators will gain instant access to system and support compliance, case reporting, ability to update and create cases, have visibility to when the system will be updated, and receive pro-active notifications regarding system updates. Available 24x7x365 from any web-enabled device, the information provided by MyView will be based on your needs and user access permissions, ensuring that the information displayed is secure and pertinent to your operations.

NOTE: For System Add On users the MyView Portal access capabilities may be limited by the System Owner.

Figure 6-1: MyView Portal offers real-time, role-based access to critical system and services information.

6.5 SERVICE STATEMENTS OF WORK

The following statement of work is applicable to the Year 1 proposed custom services and to the optionally proposed out years if purchased.

6.6 INTRODUCTION

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

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

6.6.1 Advanced Plus Services

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

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

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

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

6.6.2 Customer Support Plan (CSP)

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

The CSP is a critical component of this SOW and, once created, will automatically become integrated into this SOW by this reference. Motorola and Customer will collaborate to define the Customer-specific processes, procedures, network information, and other relevant support details required to perform the Services set forth in the Advanced Plus Services SOW.

6.6.3 Centralized Service Delivery

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

Technical Support provides telephone consultation for technical issues that require a high level of ASTRO 25 network experience and troubleshooting capabilities. Technical Support is delivered through the Motorola Solutions Support Center (SSC) by a staff of technical

support specialists skilled in diagnosis and swift resolution of infrastructure performance and operational issues. Motorola applies leading industry standards in recording, monitoring, escalating and reporting for Technical Support calls from its contracted customers, reflecting the importance of maintaining mission critical systems. Appendix B contains the SOW for Technical Support.

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

6.6.4 Field Service Delivery

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

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

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

6.6.5 Network Hardware Repair

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

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

unit is being repaired. If purchased, an appendix with the Network Hardware Repair with Advanced Replacement SOW will be included at the end of this document.

6.6.6 Security Management Operations

Remote Security Patch Installation

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

Security Monitoring

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

6.6.7 Network Updates

Network Updates Service is a comprehensive approach to technology sustainment of the ASTRO 25 system. It incorporates both software and hardware updates aligned with the ASTRO 25 platform lifecycle so the customer's system is maintained at a high level of support. Network Updates service provides a complete package of hardware, software and implementation services required to update the ASTRO 25 system with an equivalent level of functionality.

- Network Updates enable the ASTRO 25 system to function at high levels of operation over time, and allow for feature enhancement and system expansion, such as expansion of RF sites, dispatch positions, data sub-systems, network management positions, while maximizing the lifespan of the investment. Network updates provide access to the latest available standard and optional features (optional features may require an additional fee for licensing and hardware). Software and hardware updates to platform components optimize the availability of repair services support and may also provide increased capacity and processing capability. Live network updates are performed with minimal interruption to system operation and with minimal reliance on owner resources. Appendix G contains the SOW for Network Updates

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

6.6.8 MyView Portal

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

- Event Monitoring Reports: See resolution status for incidents and notifications by Incident priority level.
- Technical Support: View Incident status details to compare them to committed response times.
- OnSite Support: Observe Incident details by Incident priority level and track the progress of onsite support issue resolution.
- Annual Preventive Maintenance: Access the maintenance status for all sites and quickly identify actions needed to take to optimize system performance.
- Network Hardware Repair: Track return material authorizations (RMAs) shipped to our repair depot and eliminate the need to call for status updates.
- Security Patching: Receive automated patch downloads and status on competed updates.
- Trending Reports: Access up to 13 months of historical data and system activity to analyze Incident management.
- Asset and Contract Information: View all the assets purchased for the network, recent orders, and contract information.

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

6.7 APPENDIX A: NETWORK EVENT MONITORING STATEMENT OF WORK

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

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

1.0 Description of Network Event Monitoring Services

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

1.1 Availability

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

1.2 Geographic Availability

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

1.3 Inclusions

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

1.4 Limitations and Exclusions

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

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

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

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

1.4.3.2 System installations, upgrades, and expansions.

1.4.3.3 Customer training.

1.4.3.4 Hardware repair and/or exchange.

1.4.3.5 Network security services.

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

1.4.3.7 Information Assurance.

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

1.4.4 Reference the event catalogue to confirm monitored equipment.

1.5 Motorola has the following responsibilities:

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

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

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

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

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

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

1.5.6.1 Characterize the issue

1.5.6.2 Determine a plan of action

1.5.6.3 Assign and track the Incident to resolution.

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

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

1.6 The Customer has the following responsibilities:

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

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

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

1.6.4.1 Incident notification preferences and procedure

1.6.4.2 Repair Verification Preference and procedure

1.6.4.3 Database and escalation procedure forms.

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

1.6.5 Provide the following information when initiating a service request:

1.6.5.1 Assigned system ID number

1.6.5.2 Problem description and site location

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

1.6.6 Notify the SSC when customer performs any activity that impacts the system. (Activity that impacts the system may include, but is not limited to, installing software or hardware upgrades, performing upgrades to the network, renaming elements or devices within the network, or taking down part of the system to perform maintenance.)

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

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

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

1.6.10 Pay additional support charges above and beyond the contracted service agreements that may apply if it is determined that system faults were caused by the customer making changes to critical system parameters

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

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

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

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

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

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

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

6.7.1 Engagement Matrix

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

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

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

6.7.2 Connectivity Matrix

Request connectivity 8 weeks in advance of service start date.

System Type	Available Connectivity	Set up and Maintenance
ASTRO® 25	Internet VPN	Motorola
ASTRO® 25	T1	Motorola
ASTRO® 25	Ethernet	Motorola

Motorola Owned & Supplied Equipment Table.

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

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

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

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

6.8 APPENDIX B: TECHNICAL SUPPORT STATEMENT OF WORK

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

Motorola applies leading industry standards in recording, monitoring, escalating and reporting for Technical Support calls from its contracted customers, reflecting the importance of maintaining mission critical systems.

1.1 Description of Technical Support Services

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

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

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

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

1.2 Scope

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

1.3 Inclusions

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

1.4 Limitations and Exclusions

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

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

1.4.2 Third party support for equipment not sold by Motorola.

1.4.3 System installations, upgrades, and expansions.

1.4.4 Customer training.

1.4.5 Hardware repair and/or exchange.

1.4.6 Network security services.

1.4.7 Network transport management.

1.4.8 Motorola services not included in this statement of work.

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

1.5 Motorola has the following responsibilities:

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

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

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

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

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

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

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

1.6. The Customer has the following responsibilities:

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

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

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

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

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

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

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

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

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

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

1.7 Priority Level Definitions

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

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

1.8 Technical Support Priority Level Response Goals

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

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

6.9 APPENDIX C: NETWORK HARDWARE REPAIR STATEMENT OF WORK

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

1.1 Description of Services

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

1.2 Scope

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

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

1.3 Inclusions

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

1.4 Exclusions

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

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

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

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

1.4.4. Physically damaged infrastructure.

1.4.5. Third party equipment not shipped by Motorola

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

1.4.7 Video retrieval from Digital In-Car Video equipment.

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

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

1.4.9 Test equipment.

1.4.10. Racks, furniture and cabinets.

1.4.11. Firmware and/or software upgrades.

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

1.5 Motorola has the following responsibilities:

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

1.5.2 Provide repair return authorization numbers when requested by Customer.

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

1.5.4 Perform the following service on Motorola infrastructure:

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

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

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

1.5.4.4 Perform a box unit test on all serviced infrastructure.

1.5.4.5 Perform a system test on select infrastructure.

1.5.5 Provide the following service on select third party infrastructure:

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

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

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

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

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

defect, the repair depot reserves the right to reload infrastructure with a similar software version.

1.5.5.6 Properly package repaired infrastructure.

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

1.6 The Customer has the following responsibilities:

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

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

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

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

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

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

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

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

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

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

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

6.10 APPENDIX D: REMOTE SECURITY PATCH INSTALLATION STATEMENT OF WORK

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

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

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

1.1 Description of Remote Security Patch Installation

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

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

1.2 Connectivity

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

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

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

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

1.3 Security Update Installation

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

1.3.1 Antimalware Signature Update Installation

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

1.3.2 Microsoft Windows Security Update Installation

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

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

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

1.3.3 Microsoft Windows Security Updates Outside ASTRO 25 Firewalls

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

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

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

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

1.3.4 Quarterly Security Update Installation

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

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

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

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

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

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

1.4 Scope

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

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

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

1.5 Motorola has the following responsibilities:

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

McAfee Antivirus definitions– Weekly

Windows OS updates – Monthly

Solaris, RHEL OS, VMware ESXi updates – Quarterly

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

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

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

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

1.5.5 Pre-test STIG recommended remediation when applicable.

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

1.5.7 Coordinate updates with customer as outlined in section 1.

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

1.5.9 Notify customer of update releases by email.

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

1.6 The Customer has the following responsibilities:

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

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

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

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

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

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

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

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

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

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

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

1.7 Disclaimer:

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

6.11 APPENDIX E: ONSITE SUPPORT STATEMENT OF WORK

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

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

Description of Services

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

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

1.1 Scope

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

1.2 Inclusions

Onsite Support can be delivered on Motorola-sold infrastructure.

2.0 Motorola has the following responsibilities:

2.1. Receive service requests.

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

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

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

2.5. Servicer will perform the following on-site:

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

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

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

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

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

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

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

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

2.13.1 Open and closed; or

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

2.14. Provide Incident activity reports to customer if requested.

3.0 Customer has the following responsibilities:

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

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

3.2.1. Incident notification preferences and procedure.

3.2.2. Repair verification preference and procedure.

3.2.3. Database and escalation procedure forms.

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

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

3.3.1. Assigned system ID number.

3.3.2. Problem description and site location.

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

3.4. Allow Servicers access to equipment.

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

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

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

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

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

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

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

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

4.0 **Priority Level Definitions**

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

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

5.0 Onsite Support Priority Level Response Time Goals

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

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

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

6.12 APPENDIX F: ANNUAL PREVENTIVE MAINTENANCE STATEMENT OF WORK

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

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

1.1 Scope

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

1.2 Inclusions

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

1.3 Limitations and Exclusions

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

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

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

1.3.3. System installations, upgrades, and expansions.

1.3.4. Customer training.

1.3.5. Hardware repair and/or exchange.

1.3.6. Network security services.

1.3.7. Network transport.

1.3.8. Information Assurance.

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

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

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

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

1.4 Motorola has the following responsibilities:

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

1.4.2. Advise customer of issues that may require attention.

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

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

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

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

1.5 The Customer has the following responsibilities:

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

1.5.2. Authorize and acknowledge any scheduled system downtime.

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

1.5.4. Establish and maintain a suitable environment (heat, light, and power) for the equipment location and provide Motorola full, free, and safe access to the equipment so that Motorola may provide services. All sites shall be accessible by standard service vehicles.

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

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

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

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

1.6 The Servicer has the following responsibilities:

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

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

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

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

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

MASTER SITE CHECKLIST - LEVEL 1	
SERVERS	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diags	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
NM Client Applications	Review UEM events and transport medium types, (microwave/leased line/telco, etc). Event log review for persistent types. Verify all NM client applications are operating correctly.
Verify System SW CD's	Perform audit of software media on site. Versions, KC numbers, types, etc.
Complete Backup	Verify backups have been done or scheduled. SZ database (BAR), Centracom CDM/ADM database, etc.
Network Time Protocol (NTP)	Verify operation and syncing all devices.
Data Collection Devices (DCD) check (if present)	Verify data collection
Anti-Virus	Verify anti-virus is enabled and that definition files are up to date (within two weeks of current date) on CSMS
ROUTERS	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diags	Perform recommended diagnostic tests based on router type. Capture available diagnostic logs.
Verify Redundant Routers	Test redundancy in CWR devices. Core router switchover (coordinate with customer).
SWITCHES	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diags	Perform recommended diagnostic tests based on switch type. Capture available diagnostic logs.
Verify Redundant Switches	Test redundancy in CWR devices. Core router switchover (coordinate with customer).
DOMAIN CONTROLLERS (non-CSA)	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.

MASTER SITE CHECKLIST - LEVEL 1	
Capture Diags	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Verify System SW CD's	Perform audit of software media on site. Versions, KC numbers, types, etc.
FIREWALLS	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diags	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 Diags	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Server CPU Health	i.e. memory, HDD, CPU, disk space/utilization.

PRIME SITE CHECKLIST - LEVEL 1	
SOFTWARE	
Verify System SW CD's	Perform audit of software media on site. Versions, KC numbers, types, etc.
SWITCHES	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diags	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 Diags	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 Diags	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.

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

PRIME SITE CHECKLIST - LEVEL 1	
Site Frequency Standard Check (TRAK)	Check lights and indicators for A/B receivers.
SITE CONTROLLERS	
Capture Diags	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Clean Fans and Equipment	Use antistatic vacuum to clean cooling pathways
COMPARATORS	
Equipment Alarms	Verify no warning/alarm indicators.
Capture Diags	Perform recommended diagnostic tests based on server type. Capture available diagnostic logs.
Clean Fans and Equipment	Use antistatic vacuum to clean cooling pathways

DISPATCH SITE CHECKLIST - LEVEL 1	
GENERAL	
Inspect all Cables	Inspect all cables/connections to external interfaces are secure
Mouse and Keyboard	Verify operation of mouse and keyboard
Configuration File	Verify each operator position has access to required configuration files
Console Op Time	Verify console op time is consistent across all ops
Screensaver	Verify screensaver set as customer prefers
Screen Performance	Verify screen operational/performance
Touchscreen	Verify touchscreen operation (if applicable)
Cabling/Lights/Fans	Visual inspection of all equipment - cabling/ lights/ fans
Filters/Fans/Dust	Clean any filters/ fans/ dust- all equipment
Monitor and Hard Drive	Confirm monitor and hard drive do not "sleep"
DVD/CD	Verify / clean DVD or CD drive
Time Synchronization	Verify console time is synchronized with NTP server
Anti-Virus	Verify anti-virus is enabled and that definition files are up to date (within two weeks of current date)
HEADSET UNPLUGGED TESTING	
Speakers	Test all speakers - audio quality, volume, static, drop-outs, excess hiss when turned up.

DISPATCH SITE CHECKLIST - LEVEL 1	
Channel Audio in Speaker	Verify selected channel audio in select speaker only.
Footswitch Pedals	Verify both footswitch pedals operational
Radio On-Air Light	Verify radio on air light comes on with TX (if applicable)
HEADSET PLUGGED IN TESTING	
Radio TX and RX	Verify radio TX/RX from both headset jacks. Verify levels OK. Check volume controls for noise/static or drop-outs.
Speaker Mute	Verify select speaker muted.
Telephone Operation	Verify telephone operational through both headset jacks. Check volume controls for noise/static or drop-outs.
Audio Switches	Verify select audio switches to speaker when phone off-hook. (if interfaced to phones)
Radio Takeover in Headset	Verify radio-takeover in headset mic when phone off-hook (mic switches to radio during PTT and mutes to phone).
OTHER TESTS	
Phone Status Light	Verify phone status light comes on when phone off-hook (if applicable)
Desk Microphone Operation	Confirm desk mic operation (if applicable)
Radio IRR Operation	Verify radio IRR operational (if applicable) on MOT dispatch
Telephone IRR Operation	Verify telephone [if on radio computer] IRR operational (if applicable) on MOT dispatch
Recording	Verify operator position being recorded on long term logging recorder (if applicable) if included in service agreement
COMPUTER PERFORMANCE TESTING	
Computer Reboot	Reboot op position computer
Computer Operational	Confirm client computer is fully operational (if applicable)
AUDIO TESTING	
Conventional Resources	Confirm all conventional resources are functional with adequate audio levels and quality
Secure Mode	Confirm any secure talkgroups are operational in secure mode
Trunked Resources	Confirm all trunked resources on screen are functioning by placing a call in both directions (at the customer's discretion) and at a single op position
Backup Resources	Confirm backup resources are operational

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

RF SITE CHECKLIST - LEVEL 1	
RF PM CHECKLIST	
Equipment Alarms	Verify no warning/alarm indicators.
Clean Fans and Equipment	Use antistatic vacuum to clean cooling pathways
Site Frequency Standard Check	Check lights and indicators for A/B receivers.
Basic Voice Call Check	Voice test each voice path, radio to radio.
Control Channel Redundancy (trunking)	Roll control channel, test, and roll back.
Site Controller Redundancy (trunking) - ASR only	Roll site controllers with no dropped audio.
PM Optimization Workbook (See Table 2 for GTR tests)	Complete Base Station Verification tests - Frequency Error, Modulation Fidelity, Forward at Set Power, Reverse at Set Power, Gen Level Desense no Tx

MOSCAD CHECKLIST - LEVEL 1	
MOSCAD SERVER	
Equipment Alarms	Verify no warning/alarm indicators.
Check Alarm/Event History	Review MOSCAD alarm and events to find if there are chronic issues.
Windows Event Logs	Review Windows event logs. Save and clear if full.
Password Verification	Site devices to verify passwords. Document changes if any found.

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

FACILITIES CHECKLIST - LEVEL 1	
VISUAL INSPECTION EXTERIOR	
ASR Sign	Verify that the ASR sign is posted.
Warning Sign - Tower	Verify warning sign is posted on the tower.
Warning Sign - Gate	Verify that a warning sign is posted at the compound gate entrance.
10 Rule Sign	Verify that a 10 rules sign is posted on the inside of the shelter door.
Outdoor Lighting	Verify operation of outdoor lighting/photocell.
Exterior of Building	Check exterior of building for damage/disrepair.
Fences / Gates	Check fences/gates for damage/disrepair.
Landscape / Access Road	Check landscape/access road for accessibility.
VISUAL INSPECTION INTERIOR	
Electrical Surge Protectors	Check electrical surge protectors for alarms.
Emergency Lighting	Verify emergency lighting operation.
Indoor Lighting	Verify indoor lighting.

FACILITIES CHECKLIST - LEVEL 1	
Equipment Inspection	Visually inspect that all hardware (equipment, cables, panels, batteries, racks, etc.) are in acceptable physical condition for normal operation.
Regulatory Compliance (License, ERP, Frequency, Deviation)	Check station for regulatory compliance. Update station logs.
Clean Fans and Equipment	Use antistatic vacuum to clean cooling pathways
UPS	
Visual inspection (condition, cabling)	Verify corrosion, physical connections, dirt/dust, etc.
GENERATOR	
Visual Inspection	Verify, check panel housing, cracks, rust and weathering. Physical connections, corrosion, dirt/dust, etc.
Fuel	Verify fuel levels in backup generators, document date of last fuel delivered from fuel service provider.
Oil	Check the oil dipstick for proper level. Note condition of oil.
Verify operation (no switchover)	Check, verify running of generator, ease of start or difficult. Is generator "throttling" or running smooth? Any loud unusual noise? Etc.
Motorized Dampers	Check operation
HVAC	
Air Filter	Check air filter and recommend replacement if required.
Coils	Check coils for dirt and straightness
Outdoor Unit	Check that outdoor unit is unobstructed
Wiring	Wiring (insect/rodent damage)
Cooling / Heating	Check each HVAC unit for cooling/heating
Motorized Dampers	Check operation

MICROWAVE CHECKLIST - LEVEL 1	
GENERAL	
Transport Connectivity	Confirm transport performance by viewing UEM for site link warnings or errors.
RADIO	
Alarms	Check alarm / event history
Software	Verify version of application
TX Frequency	Verify transmit frequency

MICROWAVE CHECKLIST - LEVEL 1	
TX Power	Verify transmit power
RX Frequency	Verify receive frequency
RX Signal Level	Verify receive signal level and compare with install baseline documentation
Save configuration	Save current configuration for off site storage
Backhaul Performance	Monitor UEM status (alarms, logs, etc.) for all links. If UEM not used to monitor microwave, then use provided microwave alarm mgmt server.
WAVEGUIDE	
Visual Inspection	Inspect for wear or dents (from ground using binoculars).
Connection Verification	Verify all connections are secured with proper hardware (from ground using binoculars).
DEHYDRATOR	
Visual Inspection	Inspect moisture window for proper color
Pressure Verification	Verify pressure of all lines
Re-Pressurization	Bleed lines temporarily to verify the dehydrator re-pressurizes
Run Hours	Record number of hours ran

TOWER CHECKLIST - LEVEL 1	
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/markers are operational.
Day/Night Mode	Verify day and night mode operation.
Power Cabling	Verify that power cables are secured to tower.
ANTENNAS AND LINES	
Antennas	Visually inspect antennas for physical damage (from ground using binoculars).
Transmission Lines	Verify that all transmission lines are secure on the tower.

TOWER CHECKLIST - LEVEL 1	
GROUNDING	
Structure Grounds	Inspect grounding for damage or corrosion
GUY WIRES	
Tower Guys	Check guy wires for fraying and tension.
Guy Wire Hardware	Check hardware for rust.
CONCRETE CONDITION	
Tower Base	Check for chips or cracks.

Table 2
Site Performance Verification Procedures

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

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

6.13 APPENDIX G: NETWORK UPDATES STATEMENT OF WORK

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

1.0 Description of Service

As network updates become available, Motorola agrees to provide the customer with applicable software/hardware updates and implementation services necessary to maintain their ASTRO25 system at an exceptional level of support. ASTRO25 system software/hardware updates improve system functionality/operation and extend the useful life of the network.

1.2 Scope

This service includes 3rd Party and Motorola Solutions Software as well as select hardware to maintain supportability. All updates are pretested and certified in a dedicated ASTRO25 test lab to ensure that they are compatible and do not interfere with ASTRO25 network functionality. Network updates may also include feature enhancements. At Motorola's option, feature enhancements may be offered for purchase.

1.3 Software/Hardware under the Agreement

The ASTRO25 software covered under this agreement include:

- Base stations
- Site controllers
- Comparators
- Routers
- LAN switches
- Servers
- Dispatch consoles
- Logging equipment
- Network management terminals
- Network Fault Management ("NFM") products
- Network security devices such as firewalls and intrusion detection sensors
- Associated peripheral infrastructure software

1.3.1. Motorola Solution will provide certified hardware version updates necessary to refresh the system with an equivalent level of functionality. Any hardware versions and/or replacement hardware required to support new features or those not specifically required to maintain existing functionality are not included. Unless otherwise stated, platform migrations are not included.

1.3.2. If originally provided by Motorola, the following hardware components are eligible hardware for refresh when necessary to maintain the system functionality in place at the time this agreement was executed:

- Servers
- PC Workstations
- Routers
- LAN Switches

1.3.3. If originally provided by Motorola, the following hardware components are eligible for board-level refreshes when necessary to maintain the system functionality in place at the time this agreement was executed. A “board-level refresh” is defined as any Field Replaceable Unit (“FRU”) for the products listed below:

- GTR 8000 Base Stations
- GCP 8000 Site Controllers
- GCM 8000 Comparators
- MCC 7500 Console Operator Positions
- STR 3000 Base Stations
- Quantar Base Stations
- ASTROTAC Comparators
- PSC 9600 Site Controllers
- PBX Switches for Telephone Interconnect
- NFM/NFM XC/MOSCAD RTU

1.3.4. The parties agree that this agreement only covers those items expressly stated above. There is no coverage on any additional software or hardware products unless specifically described in this agreement. Motorola may, at its sole discretion, choose to include coverage for other items. Refer to section 1.6 for exclusions and limitations.

1.3.5. Motorola will provide implementation services necessary to install the system software and hardware updates. Any implementation services that are not directly required to support the network updates are not included. Unless otherwise stated, implementation services necessary for system expansions, platform migrations, and/or new features or functionality that are implemented concurrent with the system refresh are not included.

1.3.6. Motorola agrees to provide the necessary software design and technical resources necessary to complete the network updates.

1.3.7. The pricing in this agreement is based on the system configuration outlined in the System Pricing Configuration. This configuration is to be reviewed annually from the contract effective date. Any change in system configuration may require a price adjustment to this agreement.

1.3.8. This agreement applies only to system release version within the ASTRO25 7.X platform.

1.3.9. Motorola will issue Software Maintenance Agreement (“SMA”) bulletins on an annual basis and post them in soft copy on a designated extranet site for Customer access.

1.3.10. Any maintenance required as a result of a virus or unwanted intrusion is excluded if the system is not protected against these security threats by Motorola’s Pre-tested Security Update Service when applicable. Standard and optional features for a given ASTRO 25 system release are listed in the SMA bulletin.

1.3.11. Coverage Continuity. The parties agree that this agreement requires continuous coverage beginning within (90) days after system acceptance. Beyond (90) days from system acceptance or if payments are discontinued, additional payment(s) will be necessary to cover the period for which coverage was discontinued or delayed. The total of payments for lapses in coverage will not exceed 3 years.

1.4 **Motorola has the following responsibilities:**

1.4.1. Identify and Communicate with the customer the scope of network updates as they become available.

1.4.2. Work with the customer to schedule applicable network updates.

1.4.3. Assign the program management support required to perform network updates as necessary.

1.4.4. Assign field installation resources required to perform network updates as necessary.

1.4.5. Assign Centralized engineering resources required to perform network updates as necessary.

1.4.6. Install network updates.

1.4.7. Deliver Impact and change management training as necessary.

1.4.8. Perform appropriate system backups.

1.4.9. Work with the customer to validate that all system maintenance is current.

1.4.10. Deliver post update implementation training to the customer as needed.

1.4.11. Validate all system update deliverables are complete.

1.4.12. Obtain completion sign off from the customer.

1.5 The Customer has the following responsibilities:

1.5.1. Contact Motorola to schedule and engage the appropriate Motorola resources.

1.5.2. Customer will allow the permanent installation of a server which will be connected to Motorola and will be used for system auditing, software uploads and software update installation.

1.5.3. Asset in site walks of the system during the system audit when necessary.

1.5.4. Provide a list of any FRUs and or spare hardware to be included in the network updates when applicable.

1.5.5. Purchase any additional hardware /software necessary to implement optional system features or system expansions.

1.5.6. Provide or Purchase labor to implement optional system features or system expansions.

1.5.7. Participate in impact/Change management Training as necessary.

1.5.8. Inform system users of system updates and scheduled system downtime if necessary.

1.5.9 Cooperate with Motorola to provide post update implementation training as needed.

1.5.10 Provide Motorola with a completion sign off.

1.7 Exclusions and Limitations

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

1.7.1. This agreement does not cover any hardware or software supplied to the Customer when purchased directly from a third party, unless specifically included in this SOW.
1.7.2. This agreement does not cover software support for unauthorized modifications or other misuse of the covered software.
1.7.3. Updates for equipment add-ons or expansions during the term of this ASTRO 25 agreement are not included in the coverage of this SOW unless otherwise agreed to in writing by Motorola and Customer.

1.8 Special Provisions

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

1.9 High Speed Connectivity Specifications

1.9.1. The Minimum supported link between the core and he zone is a full T1.

1.9.2. Any link must realize or a sustain transfer rate of 17Kbps/1.4 Mbps or better bi directional.

1.9.3. Interzone Links must be fully operational when present

1.9.3. Link Reliability must satisfy these minim QoS levels:

- Port availability must meet or exceed 99.9% (three nines)
- Round trip network delay must be 100 ms or less between the core and satellite (North America) and 400 ms or less for international links o Packet loss shall be no greater than 0.3%
- Network jitter shall be no greater than 2 ms.

1.9.4. The network requirements above are based on the SLA provided for sprint dedicated IP services as of April 2012. It is possible that other vendors may not be able to meet this exact SLR, so these case must be examined on a case by case basis.

System Pricing Configuration – This configuration is to be reviewed annually from the contract effective date. Any change in the system configuration may require a price adjustment.

CORE	
Master Site Configuration	0
Zones in Operation(DSR/Dark Master site)	0
Zone Features: I&D, TDMA,Telephone Interconnect,CNI,HPD,IA,POP25, Text Messaging, Outdoor Location, ISSI 8000, Infovista,KMF/OTAR.	0

RF SYSTEM	
Voice RF Sites/Simulcast Sites(Including Prime sites)	0
Repeater/Stations(FDMA)	0
Repeater/Stations(TDMA)	0
HPD RF Sites	0
HPD Stations	

DISPATCH CONSOLE SYSTEM	
Dispatch Sites	1
MCC7500 Operator Positions(VPM)	3
Conventional Channel Gateways(CCGW)	3
Conventional Site Controller(GCP 8000)	1

LOGGING SYSTEM	
Number of AIS Servers	0
Number of Voice Logging Recorder	0
Number of Logging Replay Clients	0

NETWORK MANAGEMENT/MOSCAD NFM	
Number of NM Clients	0
Number of Fault Management Clients/NFM Clients	0
Number of Fault Management RTUs	0
Number of NM Clients	0

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

6.14 APPENDIX H: NETWORK HARDWARE REPAIR WITH ADVANCED REPLACEMENT OVERVIEW

Network Hardware Repair with Advanced Replacement is a repair exchange service for Motorola and select third party infrastructure supplied by Motorola. When available, Motorola will provide customer with an advanced replacement unit(s) or Field Replacement Units (FRU's) in exchange for customer's malfunctioning equipment. Malfunctioning equipment will be evaluated and repaired by the infrastructure repair depot and returned to depot's FRU inventory upon completion of repair. For customers who prefer to maintain their existing FRU inventory they have an option to request a "Loaner" FRU while their unit is being repaired. Refer to the Advanced Exchange or Loaner Decision Process flowchart for details on the loaner process.

The Motorola authorized repair depot manages and performs the repair of Motorola supplied equipment as well as coordinating the equipment repair logistics process.

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

1.0 Description of Services

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

1.1 Scope

Repair authorizations are obtained by contacting the Solutions Support Center which is available 24 hours a day, 7 days a week. Repair authorizations can also be obtained online via Motorola Online at under Repair Status/Submit Infrastructure RA.

Motorola Online: https://businessonline.motorolasolutions.com

1.2 Inclusions

Network Hardware Repair with Advanced Replacement is available on Motorola sold infrastructure including integrated 3rd party products. Motorola will make a "commercially reasonable effort" to repair Motorola manufactured infrastructure products for seven (7) years after product cancellation.

1.3 Exclusions

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

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

1.3.2. All third party infrastructure hardware over three (3) years from product cancellation date.

1.3.3 All broadband infrastructure three (3) years from product cancellation date

1.3.4 Physically damaged infrastructure.

1.3.5 Third party equipment not shipped by Motorola.

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

1.3.7 Video retrieval from digital in-car video equipment.

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

1.3.9 Test equipment.

1.3.10. Racks, furniture and cabinets.

1.3.11. Non-standard configurations, customer-modified infrastructure and certain third party infrastructure are excluded from advanced replacement service.

1.3.11. Firmware and/or software upgrades.

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

1.4 Motorola has the following responsibilities:

1.4.1 Enable customer access to the Motorola call center which is operational 24 hours a day, 7 days per week, to create requests for advanced replacement service.

1.4.2. Use commercially reasonable efforts to maintain FRU inventory on supported platforms.

1.4.3. Provide new or reconditioned FRU's to the customer, upon request and subject to availability. The FRU will be of similar equipment and version, and will contain equivalent boards and chips, as the customer's malfunctioning FRU.

1.4.4. Load firmware/software for equipment that requires programming. The software version information must be provided for the replacement FRU to be programmed accordingly. If the customer software version/configuration is not provided, shipping times will be delayed.

1.4.5 Package and ship Advance Exchange FRU from the FRU inventory to customer specified address.

1.4.5.1. During normal operating hours of Monday through Friday 7:00am to 7:00pm CST, excluding holidays, FRU will be shipped from Motorola as soon as possible depending on stock availability and configuration requested. Motorola will pay for the shipping to the customer, unless customer requests shipments outside of standard business hours and/or carrier programs, such as weekend or next flight out (NFO) shipment. In such cases, customer will be responsible for shipping and handling charges.

1.4.5.2. When sending the advanced replacement FRU to customer, provide a return air bill in order for customer to return the customer's malfunctioning FRU. The customer's

malfunctioning FRU will become property of the Motorola repair depot or select third party and the customer will own the advanced replacement FRU.

1.4.5.3. When sending a loaner FRU to customer, Motorola will pay for outbound shipping charges. Inbound shipping to Motorola for repair is the responsibility of the customer. Motorola will repair and return the customer's FRU and will provide a return air bill for the customer to return IDO's loaner FRU. Refer to Advanced Exchange or Loaner Decision Process flowchart for the loaner process and Shipping Charges for shipping charge detail.

1.4.6. Provide repair return authorization number upon customer request for Infrastructure that is not classified as an advanced replacement or loaner FRU.

1.4.7. Provide a repair Return Authorization (RA) number so that the returned FRU can be repaired and returned to FRU stock.

1.4.8. Receive malfunctioning FRU from Customer, carry out repairs and testing and return it to the FRU stock

1.4.9. Receive malfunctioning infrastructure from customer and document its arrival, repair and return.

1.4.10. Perform the following service on Motorola infrastructure:

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

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

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

1.4.10.4. Perform a box unit test on all serviced infrastructure.

1.4.10.5. Perform a system test on select infrastructure.

1.4.11. Provide the following service on select third party infrastructure:

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

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

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

1.4.11.4. Perform a post-test after repair by Motorola, to confirm malfunctioning infrastructure has been repaired and functions properly in a Motorola system configuration, when applicable.

1.4.12. For loaner equipment, Motorola will ship repaired infrastructure to the customer specified address during normal operating hours of Monday through Friday 7:00am to 7:00pm CST, excluding holidays. FRU will be sent two-day air unless otherwise requested. Motorola will pay for such shipping, unless customer requests shipments outside of the

above mentioned standard business hours and/or carrier programs, such as NFO (next flight out). In such cases, customer will be responsible for payment of shipping and handling charges.

1.5 The Customer has the following responsibilities:

1.5.1 Contact or instruct Servicer to contact the Motorola Solutions Support Center (SSC) and request a return authorization number prior to shipping malfunctioning infrastructure or third party infrastructure named in the applicable attached exhibit.

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

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

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

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

1.5.6. Pay for shipping of Advanced Replacement or Loaner FRU from Motorola repair depot if customer requested shipping outside of standard business hours or carrier programs set forth in section 1.5.5.1. See Shipping Charges.

1.5.7. Properly package and ship the malfunctioning FRU using the pre-paid air-bill that arrived with the advanced replacement FRU. Customer is responsible for properly packaging the malfunctioning infrastructure FRU to ensure that the shipped infrastructure arrives un-damaged and in repairable condition. Customer will be subject to a replacement fee for malfunctioning FRU's not properly returned.

1.5.8. Within five (5) business days of receipt of the advanced replacement FRU from Motorola's FRU inventory, properly package customer's malfunctioning FRU and ship the malfunctioning Infrastructure to Motorola's repair depot for evaluation and repair. Customer must send the return air bill back to the repair depot in order to facilitate proper tracking of the returned infrastructure. Customer will be subject to a full replacement fee for FRU's not returned within 5 business days.

1.5.9. For Infrastructure and/or third party infrastructure repairs that are not exchanged in advance, properly package Infrastructure and ship the malfunctioning FRU, at Customer's expense and risk of loss to Motorola.

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

1.5.11. Maintain information of software/applications and firmware for re-loading of infrastructure.

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

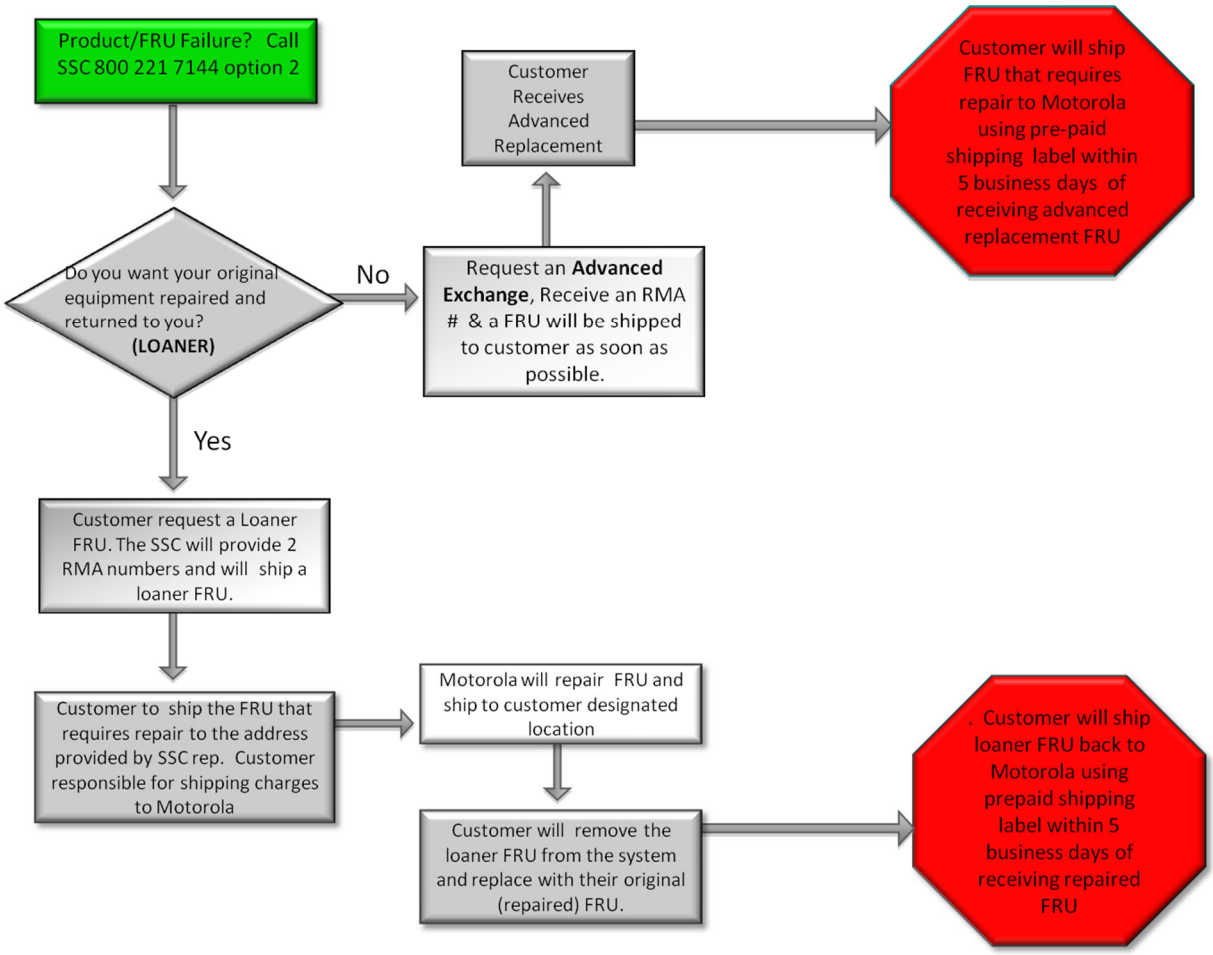

Figure 6-2: Advanced Exchange or Loaner Decision Process

Service	Advanced Replacement Contract Shipping Charges
Exchanges (Outbound to customer)	Motorola
Exchanges or Loaners Next Flight Out (Outbound to customer)	Customer
Exchanges or Loaners Non-Motorola carrier * (Outbound to customer)	Customer
Exchanges (Inbound to Motorola)	Motorola
Loaner (Outbound to customer)	Motorola
Loaner Repair (Inbound to Motorola)	Customer
Loaner Repair & Return (Outbound to customer)	Motorola
Loaner Installation (OnSite Servicer)	Customer

Figure 6-3: Shipping Charges

*Motorola shipping carriers – FedEx and DHL

6.15 APPENDIX I: SECURITY MONITORING SERVICE OVERVIEW

Motorola's Security Monitoring Services includes anti-malware monitoring and authentication log monitoring. There are also options for firewall monitoring, intrusion detection system (IDS) monitoring, and ASTRO 25 system log monitoring.

Motorola's ASTRO 25 Security Monitoring is a complete solution that provides peace of mind and reduces the risk that your network availability will be impacted by a security threat. The solution includes 24x7x365 monitoring of the radio network security elements by experienced, specialized security technologists with years of experience working with ASTRO 25 mission-critical networks. For highly complex or unusual security events, our technologists have direct and immediate access to Motorola engineers for rapid resolution.

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

1. Description of Security Monitoring Services

1.1. Anti-malware Monitoring

ASTRO 25 comes installed with Anti-malware software ("SW"). Security Monitoring will verify that malware definition updates, as provided by the Anti-malware OEM, are installed and running. The anti-malware SW is monitored for activity such as deletion, quarantine, and alerting of suspicious SW.

1.2. Authentication Monitoring

1.2.1. Active directory (including domain Linux and RADIUS) and two-factor authentication log-ins are monitored.

1.3. Firewall Monitoring – The ASTRO 25 system potentially has several firewall options. See Table 1 in the addendum for a list. In any of these firewall applications, Motorola provisions and deploys the firewalls with the ASTRO 25 system. Motorola will monitor each one that has the firewall monitoring option.

1.4. IDS (Intrusion Detection System) Monitoring. An IDS is an option to ASTRO 25 that may be deployed between the ASTRO 25 firewall and the CEN.

1.5. Centralized Log Monitoring

ASTRO 25 has an option that provides the ability to forward device syslogs to a single virtual server called Centralized Syslog Server. This allows monitoring of Linux components for authentication events.

2. Scope

The Motorola Secure Operations Center (SOC) consists of highly trained and experienced security specialists. When an event is detected, the technologists will run remote diagnostics and initiate an appropriate response. This response could involve: continuing to monitor the event for further development, attempting to remotely restore the system, or opening of an Incident for dispatch of a field servicer ("Servicer").

3. **Motorola has the following responsibilities:**

3.1. Provide, maintain, and replace when necessary, hardware ("HW") and SW required to monitor ASTRO 25 security elements. HW may include a firewall, router, or physical server. SW may include virtual servers either on the ASTRO 25 core or a separate physical server, related OS, SIEM collectors, and SW that allows distribution of updates and remote diagnostics.

3.2. Verify connectivity and monitoring is active prior to system acceptance or start date.

3.3. Coordinate with customer to maintain Motorola service authentication credentials.

3.4. Maintain properly trained and accredited technicians. Monitor the customer's system 24/7/365 for malicious or unusual activity.

3.5. Reports are posted to the SSC quality webpage. Contact your CSM for access.

4. The Customer has the following responsibilities:

4.1. Security Monitoring requires a connection from the customer's ASTRO 25 system to Motorola's SOC in Schaumburg. Motorola offers either a T1 option or a Virtual Private Network (VPN) option through a customer supplied internet connection.

4.2. Allow Motorola continuous remote access to monitor the ASTRO 25 system. This includes keeping the connection plugged-in, providing passwords, and working with Motorola to understand and maintain proper administration privileges.

4.3. Provide continuous utility service to any Motorola equipment installed or utilized at the customer's premises to support delivery of this service.

4.4. Provide customer contact information necessary to complete the Customer Support Plan. Notify your CSM within 2 weeks of any contact changes.

4.5. As necessary, upgrade the ASTRO 25 system to supported releases.

4.6. Allow Motorola dispatched-servicers physical access to the equipment when required.

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

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

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

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

5. Disclaimer

Motorola disclaims any warranty concerning the non-Motorola software and does not guarantee that customer's system will be error-free or immune to security breaches as a result of these services.

6.16 ADDENDUM

Potential ASTRO 25 Firewalls	
CNI	Customer Network Interface. This firewall separates the ASTRO 25 Radio Network from the customer's IT network (often referred to as the CEN or Customer Enterprise network). There are single and redundant (high-availability) options for the CNI, the redundant option meaning there are two firewalls. Both firewalls must be monitored in the redundant case
DSR	Dynamic System Resilience. This is an ASTRO 25 option where a geographically separated backup master site is implemented as a "hot-standby" in case of disaster at the primary. This option potentially doubles the number of firewalls in the system.
ZCP	Zone Core Protection. This ASTRO 25 option places firewalls at the master site where the RF and console sites connect. This protects the core from attack from a compromised site and propagation of the attack to the other sites. There are always 2 firewalls in this option for redundancy.
TI	Telephone Interconnect. This ASTRO 25 option allows calls to be made to/from ASTRO 25 subscribers. A firewall is required to protect the RNI from the telephone connection. One firewall may serve the dual purpose of the TI and ISSI interface.
ISSI	Inter RF Subsystem Interface. This option allows connectivity to a separate system. The original intent of this option was to connect to another P25 system supplied by either Motorola or any other P25 compliant vendor. This standard has since been used to allow connection to non-P25 systems through additional interfaces such as WAVE. In any case, a firewall is necessary to protect the RNI from this connection.
MCC 7100	The MCC 7100 dispatch console may be configured such that it can connect via Virtual Private Network (VPN) through an internet connection. A firewall is required to terminate on the ASTRO 25 side of that connection. This firewall may be physically located at either a console site or the master site and there may be multiple firewalls for this purpose.
Custom	Some customers may opt to install their own firewalls and want them monitored, most commonly at console sites. The customer will have to work with Motorola to determine if and how custom firewalls can be monitored. Additional charges may apply.

SECTION 7

PRICING SUMMARY

Description	Price
Equipment	$223,605
Implementation Services	$147,052
2019 Purchase Incentive - must order by 12/15/2019 with approval to ship immediately.	$-10,013
Total System	**$360,644**

Description – Lifecyle Services	Price
Advanced Plus Lifecycle Services – Year 2	$30,868
Advanced Plus Lifecycle Services – Year 3	$31,490
Advanced Plus Lifecycle Services – Year 4	$32,130
Advanced Plus Lifecycle Services – Year 5	$32,790

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

Terms and Conditions and Payment Schedule are per Ohio State Term Schedule 573077-0.

- 100% of equipment is due upon delivery of 100% of the equipment
- 100% of the services are due upon completion of the services
- If Post Warranty Maintenance is purchased – Motorola will invoice Customer annually in advance of each year of the plan
- Payment due Net 30 days from receipt of invoice