**`ARLINGTON COUNTY, VIRGINIA**

**AGREEMENT NO. 16-128-SS**
**AMENDMENT NUMBER 2**

This Amendment Number 2 is made on September 19, 2023 and amends Agreement Number 16-128-SS dated December 31, 2015, ("Main Agreement") between Motorola Solutions, Inc. ("Contractor") and the County Board of Arlington County, Virginia ("County").

The County and the Contractor agree to amend the Main Agreement as follows:

I. **CONTRACTOR SHALL PROVIDE AN UPGRADED ASTRO25 SYSTEM UPGRADE AGREEMENT II (SUAII) TO REPLACE EXHIBIT A-1 IN ACCORDANCE WITH ATTACHMENT A.**

II. **CONTRACTOR SHALL PROVIDE MDR SERVICE TO REPLACE THE SECURITY MONITORING IN EXHIBIT F IN ACCORDANCE WITH ATTACHMENT A.**

III. **CONTRACTOR SHALL PROVIDE A REMOTE SECURITY UPGRADE SERVICE IN ACCORDANCE WITH ATTACHMENT A.**

IV. **YEAR 9 AND YEAR 10 PRICING IN EXHIBIT B IS UPDATED TO ADD $172,329.70 IN ACCORDANCE WITH THE PRICING IN ATTACHMENT A.**

All other terms and conditions of the Main Agreement remain in effect.

WITNESS these signatures:

| THE COUNTY BOARD OF ARLINGTON COUNTY, VIRGINIA | MOTOROLA SOLUTIONS, INC. |
|---|---|
| AUTHORIZED SIGNATURE: DocuSigned by: Dr. SHARON T. LEWIS 89B86B1AD301462... | AUTHORIZED SIGNATURE: Ryan E Depp |
| NAME: DR. SHARON T. LEWIS | NAME: RYAN E. DEPP |
| TITLE: Purchasing Agent | TITLE: CUSTOMER SRVICE MANAGER |
| DATE: 9/25/2023 | DATE: 09.19.2023 |

MOTOROLA SOLUTIONS

# SERVICE AGREEMENT QUOTE ARL20230921001

*500 W. Monroe Street*
*Chicago, IL. 60661*
*(888) 325-9336*

**Service Agreement # :** TBD

Date: 9/21/2023

Required P.O.: Yes

Company Name: Arlington County, VA
Attn: Stuart Sanz
Billing Address: 1425 N. Courthouse Road, 7th Floor
City, State, Zip: Arlington County, VA 22201
Customer Contact: Stuart Sanz
Phone: 703-228-7553
Fax:

Customer # : 1035069964
Bill to Tag # : 0001
Contract Start Date: 07/01/2023
Contract End Date: 06/30/2025
Payment Cycle: Quarterly
Tax Exempt: Yes
PO # :

| Qty | Model/Option | Description | | Extended |
|---|---|---|---|---|
| | MDR | **ActiveEye Managed Detection and Response for ASTRO 25 (ActiveEye MDR pricing is in addition to the existing Security** | | |
| | | | **FY24** | $ 52,518.40 |
| | | | **FY25** | $ 55,686.49 |
| | RSUS | **Remote Security Update Service** | | |
| | | | **FY24** | $ 31,326.24 |
| | | | **FY25** | $ 32,798.57 |
| | | | **TOTAL** | **$ 172,329.70** |
| | | | **TAXES** | **N/A** |
| | | | **GRAND TOTAL** | **$ 172,329.70** |

SPECIAL INSTRUCTIONS

This Service Agreement Quote provides the pricing increase to the existing Security Monitoring on Agreement No. 16-128, dated December 18, 2015.

Terms and conditions based on Agreement No. 16-128, dated December 18, 2015, attached Cyber Terms and Conditions, and the attached ActiveEye Managed Detection and Response for ASTRO 25 Statement of Work and ASTRO25 Remote Security Update Service Statement of Work (dated May 2022)

MDR Service SoW will replace the Security Monitoring Service SoW. MDR section 1.5.2 is updated per agreement removing data storage outside the U.S. language. Clause- under section 1.5 Limitations and Exclusions of the MDR SoW is also modified.

THIS SERVICE AMOUNT IS SUBJECT TO STATE & LOCAL TAXING JURISDICTIONS, TO BE VERIFIED BY MOTOROLA.

| SUBCONTRACTORS | CITY | STATE |
|---|---|---|
| MOTOROLA SYSTEM SUPPORT CENTER | Elgin | IL |
| MOTOROLA SSC NETWORK SECURITY | Schaumburg | IL |
| MOTOROLA SYSTEM SUPPORT CENTER-NETWORK MGMT | Schaumburg | IL |
| MOTOROLA SYSTEM SUPPORT CTR-CALL CENTER | Schaumburg | IL |
| MOTOROLA SYSTEM SUPPORT-TECHNICAL SUPPORT | Schaumburg | IL |

## *Cyber Services / Opt-In Acknowledgement Section:*

***Note:** This section is to be completed by the CSM, in conjunction and cooperation with the Customer during dialog.*

| | Opt-In: Service Included In this Contract? | *Service Opt-Out? | ** Not Applicable (add reason code) |
|---|---|---|---|
| **Security Update Service (SUS)** | X | ☐ | #_____ |
| **Remote Security Update Service (RSUS)** | X | ☐ | #_____ |
| **Managed Detection and Response (MDR)** | X | ☐ | #_____ |

*** Service Opt-Out – I have received a briefing on this service and choose not to subscribe.**

**** If Selecting "Not Applicable", please consider the following, and enter a reason code:**

**1 -------Infrastructure / Product / Release Not Supported**

**2 -------Tenant or User Restrictions**

**3 -------Customer Purchased / Existing Service(s)**

---

**I have received Applicable Statements of Work which describe the Services and cybersecurity services provided on this Agreement. Motorola's Terms and Conditions, including the Cybersecurity Online Terms Acknowledgement, are attached hereto and incorporate the Cyber Addendum (available at https://www.motorolasolutions.com/en_us/managed-support-services/cybersecurity.html) by reference. By signing below Customer acknowledges these terms and conditions govern all Services under this Service Agreement.**

| AUTHORIZED CUSTOMER SIGNATURE | TITLE | DATE |
|---|---|---|
| CUSTOMER (PRINT NAME) | | |
| | Customer Service Manager | 09.21.2023 |
| MOTOROLA REPRESENTATIVE (SIGNATURE) | TITLE | DATE |
| Ryan Depp | +1 (301)-758-8059 | |
| MOTOROLA REPRESENTATIVE (PRINT NAME) | PHONE | |

MOTOROLA SOLUTIONS

# STATEMENT OF WORK

# ASTRO 25 SYSTEM UPGRADE AGREEMENT II (SUA II)

## 1.0 Description of Service and Obligations

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

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

1.3 ASTRO 25 system releases are intended to improve the system functionality and operation from previous releases and may include some minor feature enhancements. At Motorola's option, system releases may also include significant new feature enhancements that Motorola may offer for purchase. System release software and hardware shall be pre-tested and certified in Motorola's Systems Integration Test lab.

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

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

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

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

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

reprogramming are excluded from the ASTRO 25 SUA II coverage.

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

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

- 1.10.1 Servers
- 1.10.2 PC Workstations
- 1.10.3 Routers
- 1.10.4 LAN Switches

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

- 1.11.1 GTR 8000 Base Stations
- 1.11.2 GCP 8000 Site Controllers
- 1.11.3 GCM 8000 Comparators
- 1.11.4 MCC 7500 Console Operator Positions
- 1.11.5 STR 3000 Base Stations
- 1.11.6 Quantar Base Stations
- 1.11.7 Centracom Gold Elite Console Operator Interface Electronics
- 1.11.8 Centracom Gold Elite Central Electronics Banks
- 1.11.9 Ambassador Electronics Banks
- 1.11.10 Motorola Gold Elite Gateways
- 1.11.11 ASTROTAC Comparators
- 1.11.12 PSC 9600 Site Controllers
- 1.11.13 PBX Switches for Telephone Interconnect
- 1.11.14 NFM/NFM XC/MOSCAD RTU

1.12 The ASTRO 25 SUA II does not cover all products. Refer to section 2.0 for exclusions and limitations.

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

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

- 1.14.1 Review infrastructure system audit data as needed.
- 1.14.2 Identify additional system equipment needed to implement a system release, if applicable.
- 1.14.3 Complete a proposal defining the system release, equipment requirements, installation plan, and

impact to system users.

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

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

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

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

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

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

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

## 2.0 Upgrade Elements and Corresponding Party Responsibilities

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

2.1.1 Motorola responsibilities

2.1.1.1 Obtain and review infrastructure system audit data as needed.

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

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

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

2.1.1.5 Inform Customer of high speed internet connection requirements.

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

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

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

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

2.1.2 Customer responsibilities

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

2.1.2.2 Provide high-speed internet connectivity at the zone core site(s) for use by Motorola to

perform remote upgrades and diagnostics. Specifications for the high-speed connection are provided in Appendix D. High-speed internet connectivity must be provided at least 12 weeks prior to the scheduled upgrade. In the event access to a high-speed connection is unavailable, Customer may be billed additional costs to execute the system release upgrade.

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

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

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

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

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

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

2.2.1 Motorola responsibilities

2.2.1.1 Perform appropriate system backups.

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

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

2.2.2 Customer responsibilities

2.2.2.1 Validate system maintenance is current.

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

2.3 System Upgrade

2.3.1 Motorola responsibilities

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

2.3.2 Customer responsibilities

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

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

2.4 Upgrade Completion

2.4.1 Motorola responsibilities

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

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

2.4.1.3 Obtain upgrade completion sign off from the customer.

2.4.2 Customer Responsibilities

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

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

2.4.2.3 Provide Motorola with upgrade completion sign off.

## 3.0 Exclusions and Limitations

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

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

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

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

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

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

## 4.0 Special provisions

4.1 Customer acknowledges that if its System has a Special Product Feature, additional engineering may be required to prevent an installed system release from overwriting the Special Product Feature. Upon request, Motorola will determine whether a Special Product Feature can be incorporated into a system release and

whether additional engineering effort is required. If additional engineering is required Motorola will issue a change order for the change in scope and associated increase in the price for the ASTRO 25 SUA II.

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

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

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

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

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

## Appendix A – ASTRO 25 System Release Upgrade Paths

| Platform Release | Certified Upgrade Paths | |
|---|---|---|
| **Pre-7.7** | **Upgrade to Current Release** | |
| **7.7** | | |
| **7.8** | | |
| **7.9** | | |
| **7.11** | NA | 7.14 |
| **7.13** | 7.14 | 7.15 |
| **7.14** | 7.15 | 7.16 |
| **7.15** | 7.16 | 7.17 |
| **7.16** | 7.17 | 7.18 (Planned) |
| **7.17** | 7.18 (Planned) | 7.19 (Planned) |

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

## Appendix B - System Pricing Configuration

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

| | |
|---|---|
| Core | |
| Master Site Configuration | 1 M3 |
| Zones in Operation (Including DSR and Dark Master Sites) | 1 |
| Zone Features: IV&D, TDMA, Telephone Interconnect, CNI, HPD, CSMS, IA, POP25, Text Messaging, Outdoor Location, ISSI 8000, InfoVista, KMF/OTAR | 1 |
| RF System | |
| Voice RF Sites & RF Simulcast Sites (including Prime Sites) | 7 |
| Repeaters/Stations (FDMA) | 113 |
| Repeaters/Stations (TDMA) | 0 |
| HPD RF Sites | 0 |
| HPD Stations | 0 |
| Dispatch Console System | |
| Dispatch Sites | 2 |
| Gold Elite Operator Positions | 0 |
| MCC 7500 Operator Positions (GPIOM) | 0 |
| MCC 7500 Operator Positions (VPM) | 18 |
| Conventional Channel Gateways (CCGW) | 2 |
| Conventional Site Controllers (GCP 8000 Controller) | 0 |
| Logging System | |
| Number of AIS Servers | 1 |
| Number of Voice Logging Recorder | See Appendix E |
| Number of Logging Replay Clients | See Appendix E |
| Network Management and MOSCAD NFM | |
| Network Management Clients | 4 |
| MOSCAD NFM Systems | 1 |
| MOSCAD NFM RTUs | 7 |
| MOSCAD NFM Clients | 4 |
| Fire Station Alerting (FSA) | |
| FSA Systems | 0 |
| FSA RTUs | 0 |
| FSA Clients | 0 |
| Fire Station Alerting (FSA) | |
| Voice Subscribers non-APX | 0 |
| Voice Subscribers APX | 0 |
| HPD Subscribers | 0 |
| Computing and Networking Hardware (for SUA / SUA II, actual replacement qty may be less than shown) | |
| Workstations - High Performance | 8 |
| Workstations - Mid Performance | 19 |
| Servers - High Performance | 4 |
| Servers - Mid Performance | 0 |
| LAN Switch - High Performance | 3 |
| LAN Switch - Mid Performance | 18 |

| | |
|---|---|
| Routers | 21 |

**Appendix C – Security Update Service (SUS) Statement of Work**

Please see attached ASTRO 25 Security Update Service Statement of Work

**Appendix D – High-Speed Connectivity Specifications**

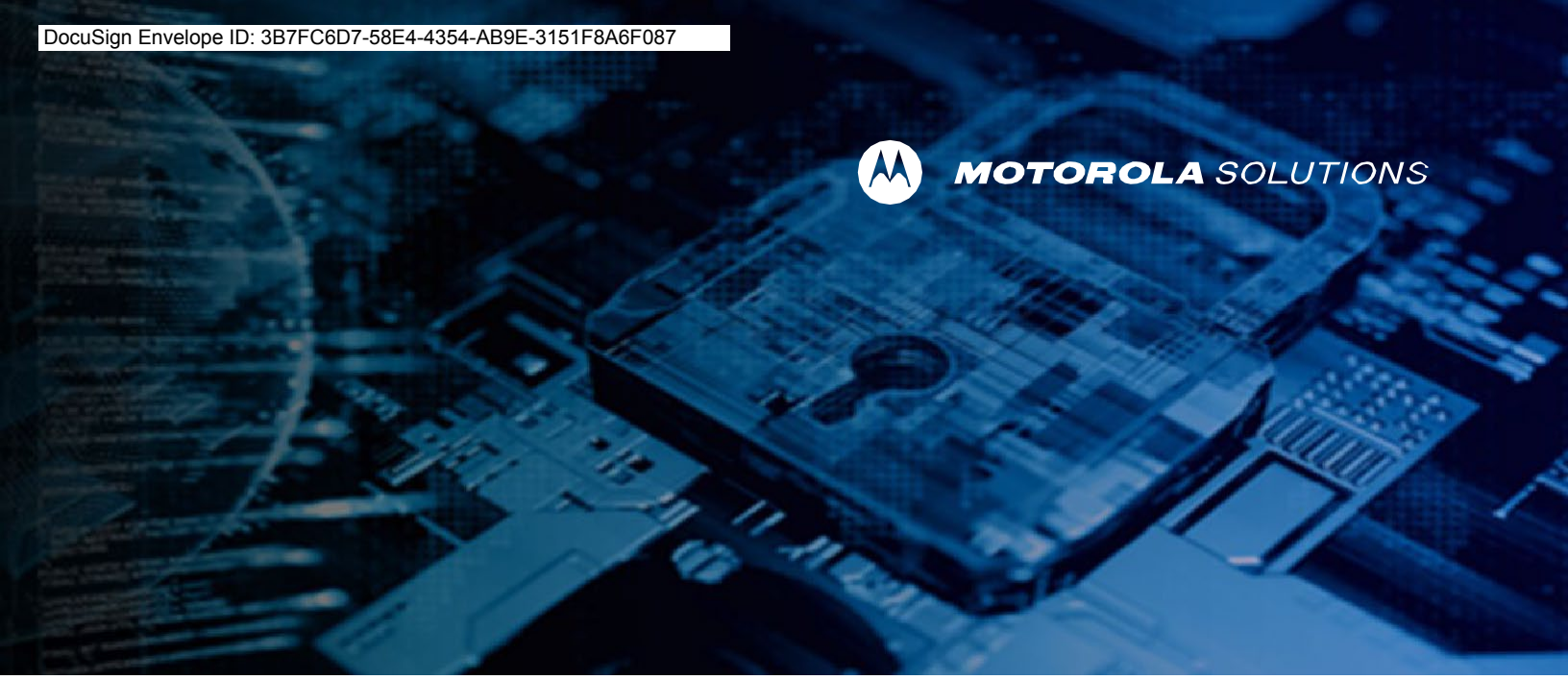
**Connectivity Requirements**

- The minimum supported link between the core and the zone is a full T1
- Any link must realize or a sustained transfer rate of 175 kBps / 1.4 Mbps or better, bidirectional
- Interzone links must be fully operational when present
- Link reliability must satisfy these minimum 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
- The network requirements above are based on the SLA provided for Sprint Dedicated IP Services as of April, 2012. It is possible other vendors may not be able to meet this exact SLA, so these cases must be examined on a case-by-case basis.

**Appendix E – NICE Configuration Detail**

This SUA II quote incorporates the following products in a multi-year SUA II Program

- One IP Radio Logger, hardware and software
- One Full Inform System with Reconstruction, Organizer and Evaluator, hardware and software
- Two NRX Telephone Loggers (64 channels each)
- ANI/ALI Interface
- Contact Closure
- CastleRock SNMP Management
- Storage Center Software
- One NAS Storage Device
- One Full Inform System Resiliency Server Hardware (Inform Software Upgrades included on the Primary Site Quote)
- One 84 Channel NRX Telephone Logger
- ANI/ALI Interface
- Contact Closure
- CastleRock SNMP Management




# ActiveEye Managed Detection and Response for ASTRO 25 Statement of Work

December 7, 2022

# Table of Contents

Section 1

# ActiveEye Managed Detection and Response for ASTRO 25 Statement of Work

## 1.1 Overview

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

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

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

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

## 1.2 Description of Service

MDR is performed by Motorola Solutions' Security Operations Center (SOC) using the ActiveEye℠ security platform. The SOC's cybersecurity analysts monitor for alerts 24x7x365. If a threat is detected, analysts will investigate and initiate an appropriate Customer engagement. Customer engagements may include, but are not limited to; requesting additional information from the Customer, continuing to monitor the event for further development, or informing the Customer to enact the Customer's documented Incident Response plan.

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

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

## 1.2.1 Managed Detection and Response Elements

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

### 1.2.1.1 ActiveEye Security Platform

Motorola Solutions' ActiveEye℠ security platform collects and analyzes security event streams from ActiveEye Remote Security Sensors (AERSS) in the Customer's ASTRO 25 network and applicable CEN systems, using security orchestration and advanced analytics to identify the most important security events from applicable systems.

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

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

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

### 1.2.1.2 ActiveEye Remote Security Sensor

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

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

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

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

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

### 1.2.1.3 Internetworking Firewall

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

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

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

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

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

## 1.2.2 Deployment Timeline and Milestones

To begin the service, an AERSS must be installed, configured, and commissioned. Motorola Solutions and the Customer will collaborate in order for the deployment tasks to be completed.

### Phase 1: Information Exchange

After contract execution, Motorola Solutions will schedule a service kick-off meeting with the Customer and provide information-gathering documents. This kick-off meeting is conducted remotely at the earliest, mutually available opportunity. Customer is to identify and ensure participation of key team members in kickoff and project initiation activities.

### Phase 2: Infrastructure Readiness

Motorola Solutions will provide detailed requirements regarding Customer infrastructure preparation actions after kick-off meeting. It is the Customer's responsibility to accomplish all agreed upon infrastructure preparations.

### Phase 3: System Buildout and Deployment

Motorola Solutions will build and provision tools in accordance with the requirements of this proposal and consistent with information gathered in earlier phases. Motorola Solutions will also provide detailed requirements regarding Customer deployment actions.

### Phase 4: Monitoring "Turn Up"

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

### Phase 5: Tuning/Report Setup

Motorola Solutions will conduct initial tuning of events and alarms in the service, and conduct ActiveEye training.

## 1.2.3 General Responsibilities

### 1.2.3.1 Motorola Solutions Responsibilities

- Provide, maintain, and when necessary repair under warranty hardware and software required to remotely monitor the ASTRO 25 network and applicable CEN systems inclusive of the AERSS and all software operating on it.
  - If the Centralized Event Logging feature is not installed on the Customer's ASTRO 25 RNI, Motorola Solutions will install it as part of this service.
- Coordinate with the Customer on any system changes necessary to integrate the AERSS into the system and establish necessary connectivity.
- Provide software and licenses to the Customer necessary to remotely monitor the ASTRO 25 network and applicable CEN environments.
- Verify connectivity and monitoring is active prior to start of service.
- Coordinate with the Customer to maintain Motorola Solutions service authentication credentials.
- Maintain trained and accredited security analysts.
- Monitor the Customer's ASTRO 25 network and applicable CEN systems 24/7/365 for malicious or unusual activity.
- Respond to security incidents in the Customer's system in accordance with Section 1.3.6: Managed Detection and Response Priority Level Definitions and Response Times. This may include, but is not limited to, requesting additional information from the Customer, continuing to monitor the event for further development or informing the Customer to enact the Customer's documented Incident Response plan.
- Assist the Customer with identifying devices that support logging within the ASTRO 25 network and applicable CEN systems have been configured to forward Syslog events to the AERSS.
- Provide the Customer with access to the ActiveEye platform enabling Customer access to security event and incident details.

### 1.2.3.2 Customer Responsibilities

- The ASTRO 25 MDR service requires a connection from the Customer's ASTRO 25 network and applicable CEN systems to the Internet. Establish connectivity with sufficient bandwidth before the service commences. Internet service bandwidth requirements are as follows:
  - Bandwidth throughput 10 MB
  - High availability Internet Connection (99.99% (4-9s) or higher).

  - Packet loss < 0.5%.
  - Jitter <10 ms.
  - Delay < 120 ms.
  - RJ45 Port Speed - Auto Negotiate
- Allow Motorola Solutions continuous remote access to monitor the ASTRO 25 network and applicable CEN systems. This includes keeping the connection active, providing passwords, and working with Motorola Solutions to understand and maintain administration privileges.
- Maintain an active Security Update Service (SUS) subscription, ensuring patches and antivirus definitions are applied according to the release cadence of the service.
- Provide continuous utility service(s) to any equipment installed or utilized at the Customer's premises to support service delivery and remote monitoring.
- Provide Motorola Solutions with contact information necessary to complete the Customer Support Plan (CSP). Notify the Customer's Customer Support Manager (CSM) within two weeks of any contact information changes.
- Notify Motorola Solutions if any components are added to or removed from the environment as it may be necessary to update or incorporate in Managed Detection and Response. Changes to monitored components may result in changes to the pricing of the MDR service.
- As necessary, upgrade the ASTRO 25 system, on-site systems, and utilize third party software or tools to supported releases.
- Allow Motorola Solutions dispatched field service technicians physical access to monitoring hardware when required.
- Cooperate with Motorola Solutions and perform all acts that are required to enable Motorola Solutions to provide the services described in this SOW.
- Configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a port(s) on a switch) network traffic to the ActiveEye sensor for applicable CEN systems.
- Responding to Cybersecurity Incident Cases created by the Motorola Solutions Security Operations Center.

## 1.2.4 Service Modules

### 1.2.4.1 Log Collection / Analytics

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

#### Motorola Solutions Responsibilities

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

### Customer Responsibilities

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

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

#### 1.2.4.2 Network Detection

Network Detection is applicable to the RNI (subject to the Customer having a Juniper IDS appliance with the appropriate IDS license(s)) and CEN.

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

### Motorola Solutions Responsibilities

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

### Customer Responsibilities

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

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

# 1.3 Security Operations Center Monitoring and Support

## 1.3.1 Scope

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

Motorola Solutions' SOC is staffed with security experts who will use ActiveEye Security Management Platform to monitor elements integrated by service modules. In addition, SOC staff will take advantage of their extensive experience to investigate and triage detected threats, and to recommend responses to the Customer.

Motorola Solutions will start monitoring the ASTRO 25 MDR service in accordance with Motorola Solutions processes and procedures after deployment, as described in Section 1.2.2: Deployment Timeline and Milestones.

The SOC receives system-generated alerts 24x7, and provides the Customer with a toll-free telephone number and email address for support requests, available 24x7. Support requests are stored in a ticketing system for accountability and reporting. The SOC will respond to detected events in accordance with Section 1.3.6: Managed Detection and Response Priority Level Definitions and Response Times.

## 1.3.2 Ongoing Security Operations Center Service Responsibilities

### Motorola Solutions Responsibilities

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

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

### Customer Responsibilities

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

## 1.3.3 Technical Support

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

### Motorola Solutions Responsibilities

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

### Customer Responsibilities

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

### Limitations and Exclusions

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

## 1.3.4 Incident Response

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

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

### Motorola Solutions Responsibilities

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

### Customer Responsibilities

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

## 1.3.5 Event Response and Notification

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

**Table 1-1: Event Handling**

| Event Type | Details | Notification Requirement |
|---|---|---|

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

## Notification

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

**Table 1-2: Notification Procedures**

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

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

## Tuning

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

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

## Tuning Period Exception

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

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

### 1.3.6 Managed Detection and Response Priority Level Definitions and Response Times

**Table 1-3: Priority Level Definitions and Response Times**

| Incident Priority | Incident Definition | Response Time |
|---|---|---|
| **Critical P1** | Security incidents that have caused, or are suspected to have caused significant and/or widespread damage to the functionality of the Customer's ASTRO 25 system or information stored within it. Effort to recover from the incident may be significant.<br>Examples:<br>• Malware that is not quarantined by anti-virus<br>• Evidence that a monitored component has communicated with suspected malicious actors. | Response provided **24 hours, 7 days** a week, including US Holidays. |
| **High P2** | Security incidents that have localized impact, but are viewed as having the potential to become more serious if not quickly addressed. Effort to recover from the incident may be moderate to significant.<br>Examples:<br>• Malware that is quarantined by antivirus.<br>• Multiple behaviors observed in the system that are consistent with known attacker techniques. | Response provided **24 hours, 7 days** a week, including US Holidays. |
| **Medium P3** | Security incidents that potentially indicate an attacker is performing reconnaissance or initial attempts at accessing the system. Effort to recover from the incident may be low to moderate.<br>Examples include:<br>• Suspected unauthorized attempts to log into user accounts.<br>• Suspected unauthorized changes to system configurations, such as firewalls or user accounts.<br>• Observed failures of security components.<br>• Informational events.<br>• User account creation or deletion.<br>• Privilege change for existing accounts. | Response provided Monday through Friday **8 am to 5 pm** local time, excluding US Holidays. |
| **Low P4** | These are typically administrative service requests from the Customer. | Response provided Monday through Friday **8 am to 5 pm** local time, excluding US Holidays. |

# 1.4 Included Services

## Site Information

The following quantities are included in the scope:

| Site / Location | Quantity |
|---|---|
| Master Site | 1 |
| DSR | 0 |
| CEN (control room, co-located, remote) | 1 |
| Network Management Clients | 4 |
| Dispatch Consoles | 28 |
| AIS | 1 |

### Services Included

The ActiveEye service modules included in our proposal are viewable in the Subscribed column below. The Network Environment column designates the location of each module: ASTRO 25 RNI, CEN, or the Control Room CEN.

| Service Module | Capabilities Included | Network Environment | Subscribed |
|---|---|---|---|
| ActiveEye Remote Security Sensor (AERSS) | Number of sensors: 2<br>• (1) CEN<br>• (1) Master Site | RNI, CEN | Yes |
| Log Collection / Analytics | Online Storage Period: 30 Day Storage<br><br>Extended Log Storage Length: 12 Months | RNI, CEN | Yes |
| Network Detection | Up to 1 Gbps per sensor port | RNI, CEN | Yes |

The following table lists any ancillary components included.

| Description | Quantity |
|---|---|
| Internetworking Firewall | 1 |

# 1.5 Limitations and Exclusions

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

Motorola Solutions' scope of services does not include responsibilities relating to active protection of customer data, including its transmission to Motorola, recovery of data available through the products or services, or remediation or responsibilities relating to the loss of data, ransomware, or hacking.

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

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

### 1.5.1 Service Limitations

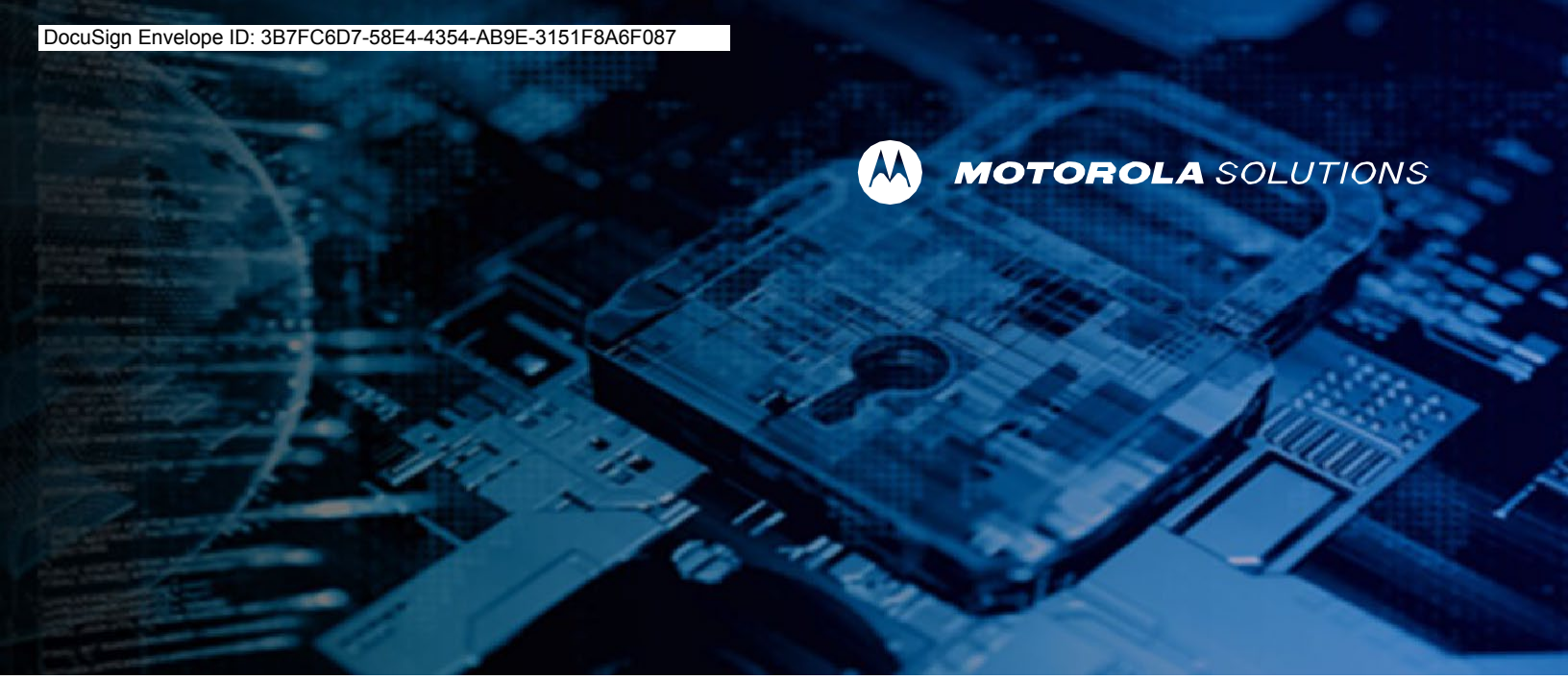
Cybersecurity services are inherently limited and will not guarantee that the Customer's system will be error-free or immune to security breaches as a result of any or all of the services described in this SOW. Motorola Solutions does not warrant or guarantee that this service will identify all cybersecurity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

### 1.5.2 Processing of Customer Data in the United States and/or other locations.

Customer understands and agrees that data obtained, accessed, or utilized in the performance of the services may be transmitted to, accessed, monitored, and/or otherwise processed by Motorola Solutions in the United States (US). Customer consents to and authorizes all such processing and agrees to provide, obtain, or post any necessary approvals, consents, or notices that may be necessary to comply with applicable law.

### 1.5.3 Customer and Third-Party Information

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




**Proposal**

# ASTRO 25 Remote Security Update Service Statement of Work

May, 2022

# Table of Contents

Section 1

# ASTRO 25 Remote Security Update Service Statement of Work

## 1.1 Overview

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

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

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

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

## 1.2 Description of Service

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

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

### 1.2.1 Remote Update Requirements

An always on, reliable connection from the Customer's network to Motorola Solutions is required to enable this service. Recommended Internet bandwidth of 20 Mbps or higher. Additional hardware (such as a secure router) may be provided to deliver the services. If the Customer is unable to install the equipment or provide a suitable Internet connection, please contact your CSM to discuss options. Please note, if an existing connection is available, this may be suitable to deliver the service.

Customer systems with slow and/or unreliable remote site links may impact our ability to deliver the service.

In some instances, Motorola Technical Notices ("MTN") must be applied to enable Motorola Solutions to remotely deploy the latest security updates. MTN installation is not part of RSUS. In the event Motorola Solutions cannot deploy security updates unless one or more MTNs are installed, Motorola Solutions will communicate this to the Customer. The Customer and their Customer Support Manager ("CSM") will determine how to apply necessary MTNs. Once necessary MTNs are applied to the Customer's system, Motorola Solutions will continue to remotely deploy security updates.

Connections to other networks, herein referred to as Customer Enterprise Network ("CEN"), are delineated by firewalls. All security updates deployed by RSUS are specific to the equipment included in the ASTRO 25 radio network with only the following exceptions: Key Management Facility ("KMF") and MCC 7500e consoles.

The Customer may request, via the CSM, that Motorola Solutions remotely updates MCC 7500e consoles and KMF in the Customer's CEN as part of RSUS, or designate Customer IT resources to install the security updates. The Customer must make the appropriate configuration changes to their firewall allowing access.

### 1.2.2 Reboot Support

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

## 1.3 Scope

RSUS includes pretested security updates for the software listed in Table 1-1. This table also describes the release cadence for security updates.

**Table 1-1: Update Cadence**

| Software | Update Release Cadence |
|---|---|
| Antivirus Definition Files | Weekly |
| Microsoft Windows | Monthly |
| Microsoft Windows SQL Server | Quarterly |
| Microsoft Windows third party (i.e. Adobe Reader) | Monthly |
| Red Hat Linux (RHEL) | Quarterly |

| Software | Update Release Cadence |
|---|---|
| VMWare ESXi Hypervisor | Quarterly |
| McAfee Patch(es) | Quarterly |
| Dot Hill DAS Firmware | Quarterly |
| HP SPP Firmware | Quarterly |

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

Intrusive security updates require Customer coordination, may require hardware reboots and zone controller rolling (switching from one zone controller to the other) to fully implement. Systems with redundant zone controllers (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. While rolling the zone controllers, the system will operate in “Site trunking” mode. The Customer will need to be aware of these operational impacts, and coordinate events with users.

# 1.4 Inclusions

Supported ASTRO 25 core types and security update delivery methods are included in Table 1-2. This table indicates if Motorola Solutions will provide any RSUS optional services to the Customer. RSUS supports the current Motorola Solutions ASTRO 25 system release and aligns with the established Software Support Policy (SwSP).

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

**Table 1-2: SUS Packages**

| Service | ASTRO 25 Core Type | Included |
|---|---|---|
| Remote Security Update Service | L Core<br>M Core<br>Simplified Core | X |
| Remote Security Update Service with Reboot Support | L Core<br>M Core<br>Simplified Core | |

Responsibilities for rebooting applicable hardware are detailed in Table 1-3.

## 1.5 Motorola Solutions Responsibilities

- If required, in order to provide the services, Motorola Solutions will send to the customer a secure router and / or a Network Management Client for installation in the ASTRO system. If the Customer is unable to install, please contact your CSM who will be able to arrange for this to be completed.
- Remotely deploy patches listed in Section 1.3 on the Customer's system. Patches will be installed on the cadence described in that section.
  - As outlined in Section 1.3, coordinate and communicate with the Customer when installing updates that will require server reboots, workstation reboots, or both.
  - Install non-intrusive updates, like antivirus definitions, as released without coordination.
- In the event no security updates are released by the Original Equipment Manufacturers ("OEM") during the usual time period, Motorola Solutions will send a notice that no new security updates were deployed.

## 1.6 Limitations and Exclusions

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

# 1.7 Customer Responsibilities

- This service requires connectivity from Motorola Solutions to the Customer's ASTRO 25 system. If required, procure internet connectivity before the service commences, and maintain it for the duration of the service contract.
- Refrain from making uncertified changes to the ASTRO 25 system. Consult with Motorola Solutions before making changes to the ASTRO 25 system.
- Be aware of the operational impacts of RSUS update installation, and coordinate the update process with users.
- Coordinate any maintenance or other updates that are not part of RSUS with Motorola Solutions to minimize downtime and redundant efforts.
- Motorola Technical Notices ("MTN") must be applied to enable Motorola Solutions to remotely deploy the latest security updates.

# 1.8 Reboot Responsibilities

Microsoft Windows servers and workstations often need to be rebooted before security updates take full effect and mitigate vulnerabilities. Reboot responsibilities are determined by the specific RSUS package being purchased. Table 1-3 contains the breakdown of responsibilities. Section 1.4 indicates which services are included.

**Table 1-3: Reboot Responsibilities Matrix**

| Remote SUS Package | Motorola Solutions Responsibilities | Customer Responsibilities |
|---|---|---|
| Remote Security Update Service | • Provide a report to the Customer's main contact listing the servers or workstations which must be rebooted to ensure installed security updates become effective. | • When a security update requires a reboot, reboot servers and workstations after security updates are installed. – |
| Remote Security Update Service with Reboot Support | • When a security update requires a reboot, dispatch a technician to reboot servers and workstations after security updates are installed. | |

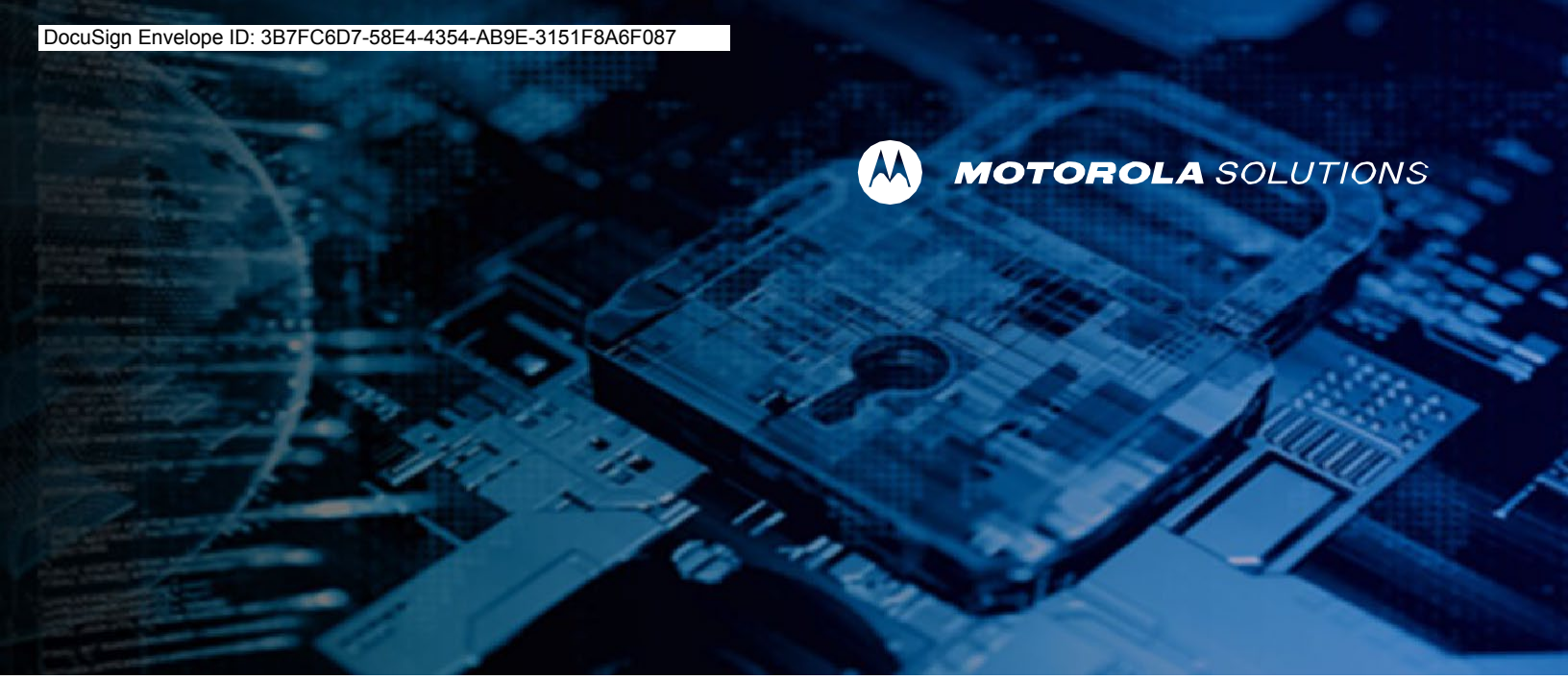
# 1.9 Disclaimer

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

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

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

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




# ASTRO 25 Security Update Service Statement of Work

January, 2022

Section 1

# ASTRO 25 Security Update Service Statement of Work

V 4.1 January, 2022

# Table of Contents

Section 1

# ASTRO 25 Security Update Service Statement of Work

## 1.1 Overview

Motorola Solutions' ASTRO® 25 Security Update Service ("SUS") provides pretested security updates, minimizing cyber risk and software conflicts. These security updates contain operating system security patches and antivirus definitions that have been validated for compatibility with ASTRO 25 systems. Security update delivery is determined by the options included as part of this service. Section 1.4 indicates if options are included as part of this service.

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

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

## 1.2 Description of Service

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

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

With the base service, the Customer will be responsible for downloading security updates, installing them on applicable components, and rebooting updated components. Additional options are available for Motorola Solutions to deploy security updates, reboot servers and workstations, or both.

### 1.2.1 On-site Delivery

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

### 1.2.2 Reboot Support

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

## 1.3 Scope

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

**Table 1-1: Update Cadence**

| Software | Update Release Cadence |
|---|---|
| Antivirus Definition Files | Weekly |
| Microsoft Windows | Monthly |
| Microsoft Windows SQL Server | Quarterly |
| Microsoft Windows third party (i.e. Adobe Reader) | Monthly |
| Red Hat Linux (RHEL) | Quarterly |
| VMWare ESXi Hypervisor | Quarterly |
| PostgreSQL<br>(From ASTRO 25 7.14 and newer major releases) | Quarterly |
| McAfee Patch(es) | Quarterly |
| Dot Hill DAS Firmware | Quarterly |
| HP SPP Firmware | Quarterly |
| QNAP Firmware | Quarterly |

## 1.4 Inclusions

Supported ASTRO 25 core types and security update delivery methods are included in Table 1-2. This table indicates if Motorola Solutions will provide any SUS optional services to the Customer. SUS supports the current Motorola Solutions ASTRO 25 system release and aligns with the established Software Support Policy (SwSP).

Motorola Solutions reserves the right to determine, which releases are supported as business conditions dictate. Additional charges may apply in the event of supporting older releases. Contact Motorola Solutions' assigned Customer Support Manager ("CSM") for the latest supported releases.

**Table 1-2: SUS Packages**

| Service | ASTRO 25 Core Type | Included |
|---|---|---|
| Security Update Service Customer Self-installed | L Core<br>M Core<br>Simplified Core | X |
| Security Update Service with Reboot Support | L Core<br>M Core<br>Simplified Core | |
| Security Update Service with On-site Delivery | L Core<br>M Core<br>Simplified Core | |

Responsibilities for downloading and installing security updates and rebooting applicable hardware are detailed in Section 1-8.

## 1.5 Motorola Solutions Responsibilities

- On the release schedule in Section 1-3`, review relevant and appropriate security patches released by Original Equipment Manufacturer (“OEM”) vendors.
- Release tested and verified security patches to Motorola Solutions’ secure website.
- Publish documentation for installation, recommended configuration changes, any identified issue(s), and remediation instructions for each security update release.
- Include printable labels the Customer may use if downloading security updates to a disk.
- Send notifications by email when security updates are available to download from the secure website.

## 1.6 Limitations and Exclusions

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

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

## 1.7 Customer Responsibilities

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

## 1.8 Installation and Reboot Responsibilities

Installation and Reboot responsibilities are determined by the specific SUS package being purchased. Table 1-3 contains the breakdown of responsibilities. Section 1-4 indicates which services are included.

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

**Table 1-3: Installation and Reboot Responsibilities Matrix**

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

# 1.9 Disclaimer

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

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

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

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