MOTOROLA SOLUTIONS

Proposal

Fulton County, Georgia

Fulton County Maintenance and SUA Renewal

March 20, 2026

PS-000188780

Motorola Solutions, Inc.
500 W Monroe Street, Suite 4400
Chicago, IL 60661

March 20, 2026

Fulton County Emergency Services
Jim Millsap, Division Chief
130 Peachtree St SW Suite 3147
Atlanta, GA 30303

Subject: Proposal for Fulton County Service and Maintenance Contract - USC000003620

Dear Chief Millsap,

Motorola Solutions is pleased to provide the attached Proposal to Fulton County to support your ASTRO P25 Radio System. This proposal is valid for 90 days from the date of this letter. We are confident that the fully integrated service solutions from Motorola Solutions, will meet the needs of Fulton County today and into the future.

We value our relationship, and are dedicated to earning your business with our commitment to provide support when and where needed. The value offered by Motorola within the scope of this Service Proposal is to provide Fulton County with manufacturer certified support on the Fulton County Public Safety Radio System, ensuring that it is maintained within the specifications needed so that you can have confidence in its performance.

Motorola has leveraged our technical and operational knowledge of Fulton County to develop a Service Proposal meeting your system and service requirements as defined in this Proposal. The proposed solution for the Maintenance and Repair of the County's Fixed Network Equipment Voice and Data Systems is designed to ensure that all equipment is operating at optimal levels at all times. This allows Fulton County to build a stronger and safer community.

We are confident that the benefits of our technical solution, as well as our corporate strength, implementation experience, and long-term service approach, offer Fulton County the peace of mind to know that you have a partner you can count on to deliver critical communications support to your First Responders and citizens. This Proposal is subject to the attached Motorola Solutions Customer Agreement and its related terms and conditions and is valid until May 18, 2025.

If you should have any questions or require additional information, please contact your account manager Mark Lee, 404-219-7011, mark.lee@motorolasolutions.com.

Sincerely,

Mark McNulty
Senior Vice President
Global Services

MOTOROLA SOLUTIONS

SERVICE AGREEMENT

500 W Monroe St
Chicago, IL 60661
(800) 247-2346

Contract Number: USC000003620
Contract Modifier: R12-FEB-2026 00:05:10

Date: 20-MAR-2026

Company Name:	Fulton County Emergency Services
Attn.:	Chief Jim Millsap
Billing Address:	130 Peachtree St Sw Ste 3147
City, State, Zip Code:	Atlanta, GA 30303
Customer Contact:	Chief Jim Millsap
Phone:	O: 404-612-8136 C: 404-734-7571

P.O.#:	Chief Jim Millsap
Customer #:	1000518673
Bill to Tag#:	0001
Contract Start Date:	01-OCT-2026
Contract End Date:	31-DEC-2034
Currency:	USD

QTY	MODEL/OPTION	SERVICES DESCRIPTION	EXTENDED AMT
		***** Recurring Services *****	
	LSV01S01109A	ASTRO SYSTEM ADVANCED PLUS PACKAGE	$7,521,479.70
	SVC01SVC0133A	COMMITTED SYSTEM MANAGER LEVEL I	$1,315,934.35
	SVC01SVC1424C	ONSITE RESPONSE-LOCAL DISPATCH-STANDARD	$96,291.99
	SVC02SVC0001C	MICROWAVE SERVICES	$464,180.02
	SVC02SVC0007C	SITE MANAGEMENT-CUSTOM SOW	$445,564.80
	SVC02SVC0018C	HVAC MAINTENANCE-CUSTOM SOW	$156,622.55
	SVC02SVC0019C	GENERATOR MAINTENANCE-CUSTOM SOW	$148,700.55
	SVC02SVC0020C	UPS MAINTENANCE-CUSTOM SOW	$898,652.98
	SVC02SVC0201A	ASTRO SUA II UO IMPLEMENTATION SERVICES	$329,849.38
	SVC02SVC0343A	RELEASE IMPACT TRAINING	$119,030.25
	SVC02SVC0344A	RELEASE IMPLEMENTATION TRAINING	$0.00
	SVC02SVC0433A	ASTRO SUA II FIELD IMPLEMENTATN SVC	$357,211.20
	SVC02SVC0493A	DCR-SUA II	$589,033.09
	SVC02SVC0496A	GENESIS-SUA II	$322,795.06
	SVC02SVC0549A	MACH SYSTEMS SUPPORT & MAINTENANCE	$486,556.30
	SVC04SVC0169A	SYSTEM UPGRADE AGREEMENT II	$2,344,545.78

	Sub Total	$15,596,448.00
	Taxes	$0.00
	Grand Total	$15,596,448.00

SPECIAL INSTRUCTIONS - ATTACH STATEMENT OF WORK FOR PERFORMANCE DESCRIPTIONS.

THIS SERVICE AMOUNT IS SUBJECT TO STATE AND LOCAL TAXING JURISDICTIONS WHERE APPLICABLE, TO BE VERIFIED BY MOTOROLA SOLUTIONS

Motorola Solutions Customer Agreement

This Motorola Solutions Customer Agreement (the "**MCA**") is entered into between Motorola Solutions, Inc., and affiliated companies, with offices at 500 W. Monroe Street, Suite 4400, Chicago, IL 60661 ("**Motorola**") and the entity purchasing Products (as defined below) from Motorola ("**Customer**"). Motorola and Customer will each be referred to herein as a "**Party**" and collectively as the "**Parties**". This Agreement (as defined below) is effective as of the earlier of (a) the first purchase of a Product from Motorola, and (b) the date of the last signature on the Agreement (the "**Effective Date**").

1. Agreement.

1.1. Scope; Agreement Documents. This MCA governs Customer's purchase of Products (as defined below) from Motorola. Additional terms and conditions applicable to specific Products are set forth in one or more agreed upon addenda incorporated within this MCA (each an "**Addendum**", and collectively the "**Addenda**"). This MCA, the applicable Addenda, and Proposal collectively form the Parties' "**Agreement**".

1.2. Order of Precedence. In interpreting this Agreement and resolving any ambiguities each Addendum will control with respect to conflicting terms in the Agreement, but only as applicable to the Products described in such Addendum. The Proposal will control with respect to conflicting terms in the MCA or any Addenda, but only as applicable to the Products and Services described in the Proposal.

2. Definitions.

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

"Change Order" means a written amendment to this Agreement after the Effective Date.

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

"Contract Price" or "**Fees**" means the charges applicable to the Products, excluding applicable sales or similar taxes and freight charges.

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

"Customer Data" has the meaning given to it in the DPA.

"**Customer-Provided Equipment**" means components, including equipment and software, not provided by Motorola which may be used with the Products.

"**Data Processing Addendum**" or "**DPA**" means the Motorola Data Processing Addendum applicable to processing of data, including Customer Data, as updated, supplemented, or superseded from time to time. The DPA is incorporated into and made a part of this Agreement for all purposes pertaining to the contents of the DPA. Where terms or provisions in the Agreement conflict with terms or provisions of the DPA, the terms or provisions of the DPA will control with respect to the contents of the DPA.

"**Delivery**" means the applicable delivery for a Product as described in Section 5.7 of this Agreement.

"Documentation" means the documentation for the Products, or data, that is delivered or made available with the Products that specifies technical and performance features, capabilities, users, or operation, including training manuals, and other deliverables, such as reports, specifications, designs, plans, drawings, analytics, or other

information.

"Equipment" means hardware provided by Motorola.

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

"Feedback" means comments or information, in oral or written form, given to Motorola by Customer or Authorized Users, including end users, in connection with or relating to the Products.

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

"Licensed Software" means software which is made available to Customer by Motorola (for example software preinstalled on Equipment, accessible via a website provided by Motorola, or software installed on or made available for Customer-Provided Equipment) and is licensed to Customer by Motorola.

"**Lifecycle Management Services**" or "**LMS**" means upgrade services as set out in the applicable Proposal.

"Maintenance and Support Services" means the break/fix maintenance, technical support, or other Services described in the applicable Proposal.

"Motorola Data" means data owned by Motorola and made available to Customer in connection with the Products;

"Motorola Materials" means proprietary equipment, hardware, content, software, tools, data, and other materials, including designs, utilities, models, methodologies, systems, and specifications, which Motorola has developed or licensed from third parties (including any corrections, bug fixes, enhancements, updates, modifications, adaptations, translations, de-compilations, disassemblies, or derivative works of the foregoing, whether made by Motorola or another party). Products, Motorola Data, Third-Party Data (as defined in the DPA), and Documentation, are considered Motorola Materials.

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

"Proposal" means solution descriptions, pricing, equipment lists, statements of work ("**SOW**"), schedules, technical specifications, quotes, order forms, and other documents setting forth the Products to be purchased by Customer and provided by Motorola. The Proposal may also include an Acceptance Test Plan ("**ATP**"); a "Payment" Form (Communications System purchase only); or a "System Acceptance Certificate" (Communications System only), depending on the Products purchased by Customer.

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

"Professional Services" are services provided by Motorola to Customer under this Agreement, including Integration Services, the nature and scope of which are more fully described in the Proposal.

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

"Services" means services, including access to services, as described in the Proposal, and includes Integration Services, Subscription Services, Professional Services, Maintenance & Support Services, and Lifecycle Management Services provided by Motorola.

"Service Completion Date" means the date of Motorola's completion of the Services described in a Proposal.

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

"Site" or **"Sites"** means the location where the Integration Services, Lifecycle Management Services, or

Maintenance and Support Services will take place.

"**Software-as-a-Service**" or "**SaaS**" means a solution that includes at least one Subscription Service and associated Licensed Software, which may include, as an example, client software or a web page.

"Software System" means a solution that includes at least one Licensed Software Product and requires Integration Services to deploy such Licensed Software Product at a Customer Site or onto any Customer-Provided Equipment or Equipment provided by or made available to Customer by Motorola.

"**Subscription**" means a recurring payment for Products, as set out in the Proposal.

"Subscription Services" or "**Recurring Services**" means Services, including access to Services, paid for on a subscription basis. Subscription Services includes services available through SaaS Products.

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

3. Products and Services.

3.1. Products. Motorola will sell (a) Equipment, (b) licenses to Licensed Software, and (c) Services to Customer, to the extent each is set forth in this Agreement. At any time during the Term, Motorola may substitute any Products at no cost to Customer, if the substitute is substantially similar to the Products set forth in this Agreement. All Licensed Software is provided pursuant to the terms of the Software License Agreement.

3.2. Services.

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

3.2.2. Integration Services; Maintenance and Support Services. Motorola will provide (a) Integration Services at the applicable Sites, agreed upon by the Parties, or (b) Maintenance and Support Services or Lifecycle Management Services, each as further described in the applicable SOW. Terms applicable to Maintenance, Support and Lifecycle Management can be found in the Maintenance, Support and Lifecycle Management Addendum.

3.2.3. Service Proposals. The Fees for Services will be set forth in Motorola's Proposal. A Customer point of contact may be set forth in the applicable SOW for the Services.

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

3.2.5. Professional Services

3.2.5.1. Additional Service Terms. If Customer is purchasing Professional Services to evaluate or assess networks, systems or operations; network security assessment or network monitoring; software application development Services; or transport connectivity services, Additional Services Terms apply.

3.3. INTENTIONALLY OMITTED

3.4. Non-Preclusion. If, in connection with the Products provided under this Agreement, Motorola performs assessments of its own, or related, products or makes recommendations, including a recommendation to purchase other products, nothing in this Agreement precludes such efforts nor precludes Motorola from participating in a future competitive bidding process or otherwise offering or selling the recommended products to Customer. Customer represents that this paragraph does not violate its procurement standards or other laws, regulations, or policies.

3.5. Customer Obligations. Customer represents that information Customer provides to Motorola in connection with receipt of Products are accurate and complete in all material respects. If any assumptions in the Proposals or information provided by Customer prove to be incorrect, or if Customer fails to perform any of its obligations under this Agreement, Motorola's ability to perform its obligations may be impacted and changes to the Agreement,

including the scope, Fees, and performance schedule may be required.

3.6. Documentation. Products may be delivered with Documentation. Documentation is and will be owned by Motorola, unless otherwise expressly stated in a Proposal that certain Documentation will be owned by Customer. Motorola hereby grants Customer a limited, royalty-free, worldwide, non-exclusive license to use the Documentation solely for its internal business purposes in connection with the Products.

3.7. Motorola Tools and Equipment. As part of delivering the Products, Motorola may provide certain tools, equipment, models, and other materials of its own. Such tools and equipment will remain the sole property of Motorola unless they are to be purchased by Customer as Products and are explicitly listed on the Proposal. The tools and equipment may be held by Customer for Motorola's use without charge and may be removed from Customer's premises by Motorola at any time without restriction. Customer will safeguard all tools and equipment while in its custody or control, and be liable for any loss or damage. Upon the expiration or earlier termination of this Agreement, Customer, at its expense, will return to Motorola all such tools and equipment in its possession or control.

3.8. Authorized Users. Customer will ensure its employees and Authorized Users comply with the terms of this Agreement and will be liable for all acts and omissions of its employees and Authorized Users. Customer is responsible for the secure management of Authorized Users' names, passwords and login credentials for access to Products.

3.9. Export Control. Customer, its employees, and any other Authorized Users will not access or use the Products in any Prohibited Jurisdiction, and Customer will not provide access to the Products to any government, entity, or individual located in a Prohibited Jurisdiction. Customer represents and warrants that (a) it and its Authorized Users are not named on any U.S. government list of persons prohibited from receiving U.S. exports, or transacting with any U.S. person; (b) it and its Authorized Users are not a national of, or a company registered in, any Prohibited Jurisdiction; (c) Customer will not permit its Authorized Users to access or use the Products or Services in violation of any U.S. or other applicable export embargoes, prohibitions or restrictions; and (d) Customer and its Authorized Users will comply with all applicable laws regarding the transmission of technical data exported from the U.S. and the country in which Customer, its employees, and the Authorized Users are located.

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

4. Term and Termination.

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

4.1.1. Subscription Terms. Unless otherwise specified in the Proposal, if the Products are purchased as a Subscription, the Subscription commences upon Delivery of, or Customer having access to, the first applicable Product ordered under this Agreement and will continue for a twelve (12) month period or such other period identified in a Proposal (the "**Initial Subscription Period**") and, unless otherwise stated in the Proposal, will automatically renew for additional twelve (12) month periods (each, a "**Renewal Subscription Year**"), unless either Party notifies the other of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. (The Initial Subscription Period and each Renewal Subscription Year will each be referred to herein as a "**Subscription Term**".) Motorola may increase Fees prior to any Renewal Subscription Year by notifying Customer of the proposed increase no later than thirty (30) days prior to commencement of the Renewal Subscription Year.

4.2. Termination. Either Party may terminate the Agreement or the applicable Addendum or Proposal if the other Party breaches a material obligation under the Agreement and does not cure such breach within thirty (30) days after receipt of notice of the breach or fails to produce a cure plan within such period of time. Each Addendum and Proposal may be separately terminable as set forth therein.

4.3. Termination for Non-Appropriation. In the event any identified funding is not appropriated or becomes

unavailable, the Customer reserves the right to terminate this Agreement for non-appropriation upon thirty (30) days' advance written notice to Motorola. In the event of such termination, Motorola shall be entitled to compensation for all conforming Products delivered or performed prior to the date of termination.

4.4. Suspension of Services. Motorola may promptly terminate or suspend any Products under a Proposal if Motorola determines: (a) the related Product license has expired or has terminated for any reason; (b) the applicable Product is being used on a hardware platform, operating system, or version not approved by Motorola; (c) Customer fails to make any payments when due; or (d) Customer fails to comply with any of its other obligations or otherwise delays Motorola's ability to perform.

4.5. Wind Down of Subscription. In addition to the termination rights in this Agreement, Motorola may terminate any Subscription Term, in whole or in part, in the event Motorola plans to cease offering the applicable Licensed Software or Subscription Services to customers.

4.6. Effect of Termination or Expiration. Upon termination for any reason or expiration of this Agreement, an Addendum, or a Proposal, Customer and the Authorized Users will return or destroy (at Motorola's option) all Motorola Materials and Motorola's Confidential Information in their possession or control and, as applicable, provide proof of such destruction, except that Equipment purchased by Customer should not be returned. If Customer has any outstanding payment obligations under this Agreement, Motorola may accelerate and declare all such obligations of Customer immediately due and payable by Customer. Notwithstanding the reason for termination or expiration, Customer agrees to pay Motorola for Products already delivered or performed. Customer has a duty to mitigate any damages under this Agreement, including in the event of default by Motorola and Customer's termination of this Agreement.

4.7. Equipment. In the event that Customer purchases any Product at a price below the published list price for such Product in connection with Customer entering into a fixed- or minimum required-term agreement for Products, and Customer or Motorola terminates the Agreement prior to the expiration of such fixed- or minimum required-term, then Motorola will have the right to invoice Customer for, and Customer will pay, the amount of the discount to the published list price for the Product or such other amount set forth in writing. This Section will not limit any other remedies Motorola may have with respect to an early termination.

5. Payment, Invoicing, Delivery and Risk of Loss

5.1. The Contract Price of $15,596,448, excluding taxes, is fully committed and identified, including all subsequent years of any contracted Services. The Customer will pay all invoices as received from Motorola subject to the terms of this Agreement and any changes in scope will be subject to the change order process as described in this Agreement.

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

5.2. Fees. Fees and charges applicable to the Products will be as set forth in the applicable Proposal. Changes in the scope of Products described in a Proposal that require an adjustment to the Fees will be set forth in the applicable pricing schedule. The Fees for any Products exclude expenses associated with unusual and costly Site access requirements (e.g., if Site access requires a helicopter or other equipment), tariffs, fluctuations in the costs of energy, raw materials, and fuel. Motorola reserves the right to equitably adjust the Fees for these expenses upon written notice to Customer. Customer will reimburse Motorola for expenses reasonably incurred by Motorola in connection with the Products. The annual Subscription Fee for Products may include certain one-time Fees, such as start-up fees, license fees, or other fees set forth in a Proposal. Motorola may suspend Licensed Software and any Subscription Services if Customer fails to make any payments within thirty (30) days of invoice due date when due.

5.3. Taxes. The Fees do not include any excise, sales, lease, use, property, or other taxes, assessments, duties, or regulatory charges or contribution requirements (collectively, "**Taxes**"), all of which will be paid by Customer, except as exempt by law, unless otherwise specified in a Proposal. If Motorola is required to pay any Taxes, Customer will reimburse Motorola for such Taxes (including any interest and penalties) within thirty (30) days after

Customer's receipt of an invoice therefore. Customer will be solely responsible for reporting the Products for personal property tax purposes, and Motorola will be solely responsible for reporting taxes on its income and net worth.

5.4. Invoicing. Motorola will invoice Customer as described in this Agreement and Customer will pay all invoices within thirty (30) days of the invoice date or as otherwise specified in writing. In the event Customer finances the purchase of the Motorola Products contemplated herein via Motorola Solutions Credit Corporation ("MSCC"), invoices for such purchase will be paid via the disbursement of the financing proceeds pursuant to the Equipment Lease - Purchase Agreement executed between the parties and the payment schedule enclosed therein shall control payment of the related invoices. Late payments will be subject to interest charges at the maximum rate permitted by law, commencing upon the due date. Motorola may invoice electronically via email, and Customer agrees to receive invoices via email at the email address set forth in Section 5.6. Customer acknowledges and agrees that a purchase order or other notice to proceed is not required for payment for Products.

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

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

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

Name_____
Address_____
Phone:_____

E-INVOICE. To receive invoices via email:

Customer Account Number_____
Customer Accounts Payable Email_____
Customer CC (optional) Email_____

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

Name_____
Address_____

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

Name_____
Address_____
Phone_____

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

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

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

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

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

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

5.10. Resale of Equipment. Equipment may contain embedded Licensed Software. If Customer desires to sell its used Equipment to a third party, Customer must first receive prior written authorization from Motorola, which will not be unreasonably denied, and obtain written acceptance of the applicable Licensed Software license terms, including the obligation to pay relevant license fees, from such third party. Customer will take appropriate security measures when disposing of Equipment, including the deletion of all data stored in the Equipment.

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

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

6.2. Site Conditions. Customer will ensure that (a) all Sites are safe and secure, (b) Site conditions meet all applicable industry and legal standards (including standards promulgated by OSHA or other governmental or regulatory bodies), (c) to the extent applicable, Sites have adequate physical space, air conditioning, and other environmental conditions, electrical power outlets, distribution, equipment, connections, and telephone or other communication lines (including modem access and interfacing networking capabilities), and (d) Sites are suitable for the installation, use, and maintenance of the Products. This Agreement is predicated upon normal soil conditions as defined by the version of E.I.A. standard RS-222 in effect on the Effective Date.

6.3. Site Issues. Upon its request, which will not be unreasonably denied, Motorola will have the right to inspect the Sites and advise Customer of any deficiencies or non-conformities with the requirements of this **Section 6 – Sites; Customer-Provided Equipment; Non-Motorola Materials**. If Motorola or Customer identifies any deficiencies or non-conformities, Customer will promptly remediate such issues or the Parties will select a replacement Site. If a Party determines that a Site identified in a Proposal is not acceptable or desired, the Parties will cooperate to investigate the conditions and select a replacement Site or otherwise adjust the installation plans and specifications as necessary. A change in Site or adjustment to the installation plans and specifications may cause a change in the Fees or performance schedule under the applicable Proposal.

6.4. Customer-Provided Equipment. Customer will be responsible, at its sole cost and expense, for providing and maintaining the Customer-Provided Equipment in good working order. Customer represents and warrants that it has all rights in Customer-Provided Equipment to permit Motorola to access and use the applicable Customer-Provided Equipment to provide the Products under this Agreement, and such access and use will not violate any laws or infringe any third-party rights (including intellectual property rights). Customer (and not Motorola) will be fully liable for Customer-Provided Equipment, and Customer will immediately notify Motorola of any Customer-Provided Equipment damage, loss, change, or theft that may impact Motorola's ability to provide the Products under this Agreement, and Customer acknowledges that any such events may cause a change in the Fees or performance schedule under the applicable Proposal.

6.5. Non-Motorola Materials. In certain instances, Customer may be permitted to access, use, or integrate Non-

Motorola Materials with or through the Products. If Customer accesses, uses, or integrates any Non-Motorola Materials with the Products, Customer will first obtain all necessary rights and licenses to permit Customer's and its Authorized Users' use of the Non-Motorola Materials in connection with the Products. Customer will also obtain the necessary rights for Motorola to use such Non-Motorola Materials in connection with providing the Products, including the right for Motorola to access, store, and process such Non-Motorola Materials (e.g., in connection with SaaS Products), and to otherwise enable interoperation with the Products. Customer represents and warrants that it will obtain the foregoing rights and licenses prior to accessing, using, or integrating the applicable Non-Motorola Materials with the Products, and that Customer and its Authorized Users will comply with any terms and conditions applicable to such Non-Motorola Materials. If any Non-Motorola Materials requires access to Customer Data, Customer hereby authorizes Motorola to allow the provider of such Non-Motorola Materials to access Customer Data, in connection with the interoperation of such Non-Motorola Materials with the Products.

6.6. Customer acknowledges and agrees that Motorola is not responsible for, and makes no representations or warranties with respect to, the Non-Motorola Materials (including any disclosure, modification, or deletion of Customer Data resulting from use of Non-Motorola Materials or failure to properly interoperate with the Products). If Customer receives notice that any Non-Motorola Materials must be removed, modified, or disabled within the Products, Customer will promptly do so. Motorola will have the right to disable or remove Non-Motorola Materials if Motorola believes a violation of law, third-party rights, or Motorola's policies is likely to occur, or if such Non-Motorola Materials poses or may pose a security or other risk or adverse impact to the Products, Motorola, Motorola's systems, or any third party (including other Motorola customers).

6.7. Motorola may provide certain Non-Motorola Materials as an authorized sales representative of a third party as set out in a Proposal. As an authorized sales representative, the third party's terms and conditions will apply to any such sales. Any orders for such Non-Motorola Materials will be fulfilled by the third party.

6.8. End User Licenses. Notwithstanding any provision to the contrary in the Agreement, certain Non-Motorola Materials software are governed by a separate license, EULA, or other agreement, including terms governing third-party equipment or software, such as open source software, included in the Products. Customer will comply, and ensure its Authorized Users comply, with any such additional terms applicable to third-party equipment or software. Certain third party flow-down terms applicable to Motorola Products may apply.

6.9. Prohibited Use. Customer will not integrate or use, or permit a third party or an Authorized User to integrate or use, any Non-Motorola Materials with or in connection with a Software System or other Licensed Software provided by Motorola under this Agreement, without the express written permission of Motorola.

6.10. API and Client Support. Motorola will use reasonable efforts to maintain its Application Programming Interfaces (APIs) for each Software System, understanding that APIs will evolve. Motorola will support each API version for 6 months after introduction but may discontinue support with reasonable notice or without notice if a security risk is present. For Licensed Software requiring a local client installation, Customer is responsible for installing the current version. Motorola will support each client version for 45 days after its release but may update the client at any time, and does not guarantee support for prior client versions.

7. Representations and Warranties.

7.1. Mutual Representations and Warranties. Each Party represents and warrants to the other Party that (a) it has the right to enter into, and execute, the Agreement and perform its obligations hereunder, and (b) the Agreement will be binding on such Party.

7.2. System Warranty. Subject to the disclaimers and exclusions below, Motorola represents and warrants that, on the date of System Acceptance (for Communications Systems), System Completion Date (for Software Systems), or Delivery, as applicable (a) the Communications System will perform in accordance with the descriptions in the applicable Proposal in all material respects, (b) the Software System will perform in accordance with the descriptions in the applicable Proposals in all material respects, and (c) if Customer has purchased any Licensed Software (but, for clarity, excluding SaaS Products) as part of such Communications System or Software System, the warranty period applicable to such Licensed Software will continue for a period of one (1) year commencing upon System Acceptance, System Completion, or date the Licensed Software is delivered (the "**Warranty Period**").

7.3. Communications Systems. During the Warranty Period, in addition to warranty services, Motorola will provide Maintenance and Support Services for the Equipment and support for the Motorola Licensed Software in Communication Systems pursuant to the applicable maintenance and support Proposal. Support for the Licensed Software will be in accordance with Motorola's established Software Support Policy ("SwSP"). If Customer wishes to purchase (a) additional Maintenance and Support Services during the Warranty Period; or (b) continue or expand maintenance, software support, installation, and/or Motorola's LMS after the Warranty Period, Motorola will provide the description of and pricing for such services in a separate proposal document and such terms will be agreed upon in a Proposal. Unless otherwise agreed by the Parties in writing, the terms and conditions of the MSLMA referenced in Section 3.2.2 will govern the provision of such Services.

7.4. SaaS. SaaS Products do not qualify for the System Warranty above.

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

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

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

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

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

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

ISSUES OR OBSOLESCENCE OF LICENSED SOFTWARE DUE TO CHANGES IN CUSTOMER OR AUTHORIZED USER REQUIREMENTS, EQUIPMENT, OR SYSTEMS; (K) TRACKING AND LOCATION-BASED SERVICES; OR (L) BETA SERVICES.

8. Indemnification.

8.1. General Indemnity. Motorola will defend, indemnify, and hold Customer harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual third-party claim, demand, action, or proceeding ("Claim") for personal injury, death, or direct damage to tangible property to the extent caused by Motorola's negligence, gross negligence or willful misconduct while performing its duties under this Agreement, except to the extent the claim arises from Customer's negligence or willful misconduct. Motorola's duties under this **Section 8.1 – General Indemnity** are conditioned upon: (a) Customer promptly notifying Motorola in writing of the Claim; (b) Motorola having sole control of the defense of the suit and all negotiations for its settlement or compromise to the extent allowed by applicable law; and (c) Customer cooperating with Motorola and, if requested by Motorola, providing reasonable assistance in the defense of the Claim.

8.2. Intellectual Property Infringement. Motorola will defend Customer against any third-party claim alleging that a Motorola-developed or manufactured Product (the "Infringing Product") directly infringes a United States patent or copyright ("Infringement Claim"), and Motorola will pay all damages finally awarded against Customer by a court of competent jurisdiction for an Infringement Claim, or agreed to in writing by Motorola in settlement of an Infringement Claim. Motorola's duties under this **Section 8.2 – Intellectual Property Infringement** are conditioned upon: (a) Customer promptly notifying Motorola in writing of the Infringement Claim; (b) Motorola having sole control of the defense of the suit and all negotiations for its settlement or compromise; and (c) Customer cooperating with Motorola and, if requested by Motorola, providing reasonable assistance in the defense of the Infringement Claim.

8.2.1. If an Infringement Claim occurs, or in Motorola's opinion is likely to occur, Motorola may at its option and expense: (a) procure for Customer the right to continue using the Infringing Product; (b) replace or modify the Infringing Product so that it becomes non-infringing; or (c) grant Customer (i) a prorated refund of any amounts pre-paid for the Infringing Product (if the Infringing Product is Licensed Software) or (ii) a credit for the Infringing Product, less a reasonable charge for depreciation (if the Infringing Product is Equipment, including Equipment with embedded Licensed Software).

8.2.2. In addition to the other damages disclaimed under this Agreement, Motorola will have no duty to defend or indemnify Customer for any Infringement Claim that arises from or is based upon: (a) Customer Data, Customer-Provided Equipment, Non-Motorola Materials, or third-party equipment, hardware, software, data, or other third-party materials; (b) the combination of the Product with any products or materials not provided by Motorola; (c) a Product designed, modified, or manufactured in accordance with Customer's designs, specifications, guidelines or instructions; (d) a modification of the Product by a party other than Motorola; (e) use of the Product in a manner for which the Product was not designed or that is inconsistent with the terms of this Agreement; or (f) the failure by Customer to use or install an update to the Product that is intended to correct the claimed infringement. In no event will Motorola's liability resulting from an Infringement Claim extend in any way to any payments due on a royalty basis, other than a reasonable royalty based upon revenue derived by Motorola from Customer from sales or license of the Infringing Product.

8.2.3. This **Section 8.2 – Intellectual Property Infringement** provides Customer's sole and exclusive remedies and Motorola's entire liability in the event of an Infringement Claim.

8.3. Customer Indemnity. To the extent allowed by applicable law, Customer will defend, indemnify, and hold Motorola and its subcontractors, subsidiaries and other affiliates harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual or threatened third-party claim, demand, action, or proceeding arising from or related to (a) Customer-Provided Equipment, Customer Data, or Non-Motorola Materials, including any claim, demand, action, or proceeding alleging that any such equipment, data, or materials (or the integration or use thereof with the Products) infringes or misappropriates a third-party intellectual property or other right, violates applicable law, or breaches the Agreement; (b) Customer-Provided Equipment's failure to meet the minimum requirements set forth in the applicable Documentation or match the applicable specifications provided to Motorola by Customer in connection with the Products; (c) Customer's (or its service providers, agents, employees, or Authorized User's) negligence or willful

misconduct; and (d) Customer's or its Authorized User's breach of this Agreement. This indemnity will not apply to the extent any such claim is caused by Motorola's use of Customer-Provided Equipment, Customer Data, or Non-Motorola Materials in violation of the Agreement. Motorola will give Customer prompt, written notice of any claim subject to the foregoing indemnity. Motorola will, at its own expense, cooperate with Customer in its defense or settlement of the claim.

9. Limitation of Liability.

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

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

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

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

10. Confidentiality.

10.1. Confidential Information. Customer and Motorola agree that, subject to any applicable freedom of information or public records legislation, Motorola's Confidentiality Terms apply to information shared between the Parties.

11. Proprietary Rights; Data; Feedback.

11.1. Motorola Materials. Customer acknowledges that Motorola may use or provide Customer with access to "Motorola Materials". Except when Motorola has expressly transferred title or other interest to Customer in writing,

the Motorola Materials are the property of Motorola or its licensors, and Motorola or its licensors retain all right, title and interest in and to the Motorola Materials (including, all rights in patents, copyrights, trademarks, trade names, trade secrets, know-how, other intellectual property and proprietary rights, and all associated goodwill and moral rights).

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

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

11.3. Feedback. Any Feedback provided by Customer is entirely voluntary, and will not create any confidentiality obligation for Motorola, even if designated as confidential by Customer. Motorola may use, reproduce, license, and otherwise distribute and exploit the Feedback without any obligation or payment to Customer or Authorized Users and Customer represents and warrants that it has obtained all necessary rights and consents to grant Motorola the foregoing rights.

11.4. Improvements; Products and Services. The Parties agree that, notwithstanding any provision of this Agreement to the contrary, all fixes, modifications and improvements to the Services or Products conceived of or made by or on behalf of Motorola that are based either in whole or in part on the Feedback, Customer Data, or Service Use Data (or otherwise) are the exclusive property of Motorola and all right, title and interest in and to such fixes, modifications or improvements will vest solely in Motorola. Customer agrees to execute any written documents necessary to assign any intellectual property or other rights it may have in such fixes, modifications or improvements to Motorola.

12. Acceptance

12.1. Communications System Acceptance**.** Unless further defined in the applicable Proposal or Statement of Work, System Acceptance for a Communications System occurs upon successful completion of Acceptance Tests as detailed in the Acceptance Test Plan. Motorola will provide ten days' notice before testing begins, and upon successful completion, both parties will sign an acceptance certificate. If the plan includes tests for subsystems or phases, acceptance occurs upon successful completion of those tests and separate certificates will be issued. If Customer believes the system has failed, they must provide a detailed written notice within thirty days; otherwise, System Acceptance is deemed to have occurred. Minor, non-material issues will not delay acceptance but will be addressed per a mutually agreed schedule. Customer use of the system before System Acceptance requires Motorola's written authorization and transfers responsibility for system operation to the Customer. Software System Completion is defined by Customer's Beneficial Use of each Product within the system, with “Beneficial Use” defined to occur thirty days after functional demonstration if not otherwise defined in the Proposal.

13. Force Majeure; Delays Caused by Customer.

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

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

for its out-of-pocket costs incurred due to the delay (including those incurred by Motorola's affiliates, vendors, and subcontractors).

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

14.1. Governing Law. All matters relating to or arising out of the Agreement are governed by the laws of the State of Illinois, unless Customer is the United States Government (or an agency thereof) or a state government or state agency or local municipality within the United States, in which case all matters relating to or arising out of the Agreement will be governed by the laws of the State in which the Products and Services are provided. The terms of the U.N. Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act will not apply.

14.2. Negotiation; Mediation. The Parties will attempt to timely resolve the Dispute promptly through good faith negotiations. Either Party may initiate dispute resolution procedures by sending a notice of Dispute ("Notice of Dispute") to the other Party. The Parties will choose an independent mediator within thirty (30) days of such Notice of Mediation. Neither Party may unreasonably withhold consent to the selection of a mediator, but if the Parties are unable to agree upon a mediator, either Party may request that the American Arbitration Association nominate a mediator. Each Party will bear its own costs of mediation, but the Parties will share the cost of the mediator equally. Unless otherwise agreed in writing, all in person meetings under this **Section 14.2 – Negotiation; Mediation** will take place in Chicago, Illinois, and all communication relating to the Dispute resolution will be maintained in strict confidence by the Parties. Notwithstanding the foregoing, any Dispute arising from or relating to Motorola's intellectual property rights must be decided by a court of competent jurisdiction, in accordance with **Section 14.3 – Litigation, Venue, Jurisdiction** below.

14.3. Litigation, Venue, Jurisdiction. If the Dispute has not been resolved by mediation within sixty (60) days from the Notice of Mediation, either Party may submit the Dispute exclusively to a court in Cook County, Illinois, or in the case the Customer is the United States, a state agency, or local municipality, then the appropriate court in the State in which the Products and Services are provided. Each Party expressly consents to the exclusive jurisdiction of such courts for resolution of any Dispute and to enforce the outcome of any mediation.

15. General.

15.1. Compliance with Laws. Each Party will comply with applicable laws in connection with the performance of its obligations under this Agreement, including that Customer will ensure its and its Authorized Users' use of the Products complies with law (including privacy laws), and Customer will obtain any FCC, FAA, and other licenses or authorizations (including licenses or authorizations required by foreign regulatory bodies) required for its and its Authorized Users' use of the Products. Motorola may, at its discretion, cease providing or otherwise modify Products (or any terms related thereto in an Addendum or Proposal), in order to comply with any changes in applicable law.

15.2. Audit; Monitoring. Motorola will have the right to monitor and audit use of the Products, including an audit of total user licenses credentialed by Customer for any Licensed Software or SaaS Products, which may also include access by Motorola to Customer Data and Service Use Data. Customer will provide notice of such monitoring to its Authorized Users and obtain any required consents, including individual end users, and will cooperate with Motorola in any monitoring or audit. Customer will maintain during the Term, and for two (2) years thereafter, accurate records relating to any licenses granted under this Agreement to verify compliance with this Agreement. Motorola or a third party ("Auditor") may inspect Customer's and, as applicable, Authorized Users' premises, books, and records. Motorola will pay expenses and costs of the Auditor, unless Customer is found to be in violation of the terms of the Agreement, in which case Customer will be responsible for such expenses and costs. In the event Motorola determines that Customer's usage of the Licensed Software or SaaS Product exceeded the number of licenses purchased by Customer at a given time, Motorola may invoice Customer for the additional licenses used by Customer, pro-rated for each additional license from the date such license was activated, and Customer will pay such invoice in accordance with the payment terms in the Agreement.

15.3. Assignment and Subcontracting. Neither Party may assign or otherwise transfer this Agreement without the prior written approval of the other Party. Motorola may assign or otherwise transfer this Agreement or any of its rights or obligations under this Agreement without consent (a) for financing purposes, (b) in connection with a merger, acquisition or sale of all or substantially all of its assets, (c) as part of a corporate reorganization, or (d) to

a subsidiary corporation. Subject to the foregoing, this Agreement will be binding upon the Parties and their respective successors and assigns. Motorola may subcontract any of the work, but subcontracting will not relieve Motorola of its duties under this Agreement.

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

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

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

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

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

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

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

15.11. Survival. The following provisions will survive the expiration or termination of this Agreement for any reason: Section 3.5 – Customer Obligations; Section 4.6 – Effect of Termination or Expiration; Section 5 – Payment and Invoicing; Section 7.9 – Warranty Disclaimer; Section 7.10 - Additional Warranty Exclusions; Section 8.3 – Customer Indemnity; Section 9 – Limitation of Liability; Section 10 – Confidentiality; Section 11 – Proprietary Rights; Data; Feedback; Section 13 – Force Majeure; Delays Caused by Customer; Section 14 – Disputes; and Section 15 – General.

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

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

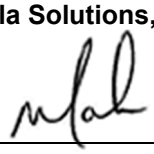
Motorola Solutions, Inc.	**Customer:** _____
By: 	By: _____
Name: Mark McNulty	Name: _____
Title: Senior Vice President	Title: _____
Date: March 20, 2026	Date: _____

Table of Contents

Section 1

ASTRO 25 Advanced Plus Services Statement of Work

1.1 Overview

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

Some Advanced Plus and third party services described in this proposal are priced for optional purchase consideration. The specific service descriptions herein are applicable only for the specific services Fulton County contracts in its Service Agreement.

Advanced Plus Services consist of the following elements:

- ASTRO System Monitoring:
  - Managed Detection and Response (MDR).
  - Network Event Monitoring.
  - ASTRO Connectivity Service (ACS) enabled for RSUS, System Monitoring.
- Remote Technical Support.
- Network Hardware Repair.
- Security Update Service (SUS).
- Remote Security Update Service (RSUS).
- On-Site Infrastructure Response.
- Annual Preventative Maintenance.
- System Upgrade Agreement (SUA).

Each of these elements is summarized below and expanded upon in Section 1.4 Advanced Plus Services Detailed Description. In the event of a conflict between the descriptions below and an individual subsection of Section 1.4 Advanced Plus Services Detailed Description, the individual subsection prevails.

Third Party Services consist of the following elements:

- Microwave Extended AviatCare Support.
- Microwave On-Site Support.
- Genesis Support and Upgrade Agreement.
- Vertiv UPS Service Agreement.
- Tower RF Site vegetation Control.

- Generator PM Support.
- HVAC PM Support.

Third party services are described in Section 1.8: Third Party Maintenance Services Detailed Description. In the event of a conflict between the Section 1.8 descriptions below and an individual subsection, the Section 5 subsection prevails.

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

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

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

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

ASTRO System Monitoring

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

- Managed Detection and Response

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

- Network Event Monitoring

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

- ASTRO Connectivity Service

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

Remote Technical Support

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

Network Hardware Repair

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

Security Update Service

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

Remote Security Update Service

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

On-Site Infrastructure Response

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

Annual Preventive Maintenance

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

System Upgrade Agreement

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

1.2 Motorola Service Delivery Ecosystem

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

1.2.1 Centralized Managed Support Operations

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

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

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

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

1.2.2 Field Service

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

1.2.3 System Manager

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

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

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

1.2.4 Customer Hub

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

- **Network Event Monitoring**: Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.
- **Remote Technical Support**: Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.
- **Network Hardware Repair**: Track return material authorizations (RMA) shipped to Motorola's repair depot and eliminate the need to call for status updates. In certain countries, customers will also have the ability to create new RMA requests online.
- **On-Site Infrastructure Response**: Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.

- **Annual Preventive Maintenance**: View incident status and details of each annual change request for preventive maintenance, including completed checklist information for the incident.
- **Network Updates**: View system status overview and software update information.
- **Managed Detection and Response**: Manage incidents and view self-service reports. Observe incident details by incident priority level, and track the progress of issue resolution.
- **Orders and Contract Information**: View available information regarding orders, service contracts, and service coverage details.

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

1.3 Connectivity Specifications

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

1.4 Advanced Plus Services Detailed Description

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

1.4.1 ASTRO System Monitoring (NEW)

1.4.1.1 Managed Detection and Response

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

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

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

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

1.4.1.1.1 Description of Service

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

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

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

1.4.1.1.2 Managed Detection and Response Elements

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

ActiveEye Security Platform

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

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

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

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

ActiveEye Remote Security Sensor

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

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

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

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

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

Endpoint Detection and Response

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

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

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

Cloud Based Vulnerability Scan Engine

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

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

Control Room Firewall

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

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

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

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

1.4.1.1.3 Deployment Timeline and Milestones

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

Phase 1: Service Onboarding

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

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

Phase 2: Infrastructure Readiness

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

Phase 3: System Buildout and Deployment

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

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

Phase 4: Monitoring "Turn Up"

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

Phase 5: Tuning and Customer Training

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

Service Commencement

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

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

1.4.1.1.4 General Responsibilities

Motorola Responsibilities

- Provide and when necessary repair under manufacturer warranty hardware and software required to remotely monitor the ASTRO 25 network and applicable CEN systems inclusive of the AERSS and all software operating on it.
  - If the Centralized Event Logging feature is not installed on the Customer’s ASTRO 25 RNI, Motorola will install it as part of this service.
- Coordinate with the Customer on any system changes necessary to integrate the AERSS into the system and establish necessary connectivity.
- Provide software and licenses to the Customer necessary to remotely monitor the ASTRO 25 network and applicable CEN environments.
- Integrate EDR agents as per the “Deployment Timeline and Milestones” section in all network segments where endpoint detection and response is in scope.
  - Note that network segments with insufficient connectivity to support endpoint detection and response will be considered out of scope for endpoint detection and response.
  - Motorola will perform the installation of endpoint detection and response agents in the RNI-DMZ CEN(s) and Control Room CEN(s) for all Motorola managed devices that support endpoint detection and response agents.
  - Motorola will support the customer with installing endpoint detection and response agents in the RNI-DMZ CEN(s) and Control Room CEN(s) for any device that supports endpoint detection and response agents and is not Motorola Solutions managed. Due to the fact that Motorola does not typically manage the devices and network connectivity for endpoints in the Control Room CEN, it is ultimately the customer’s responsibility to perform this installation.
- Assist the Customer with the installation of log forwarding agents on systems that are not managed by Motorola. Note, Motorola will perform installation on all endpoints that are managed by Motorola.
- Verify connectivity and monitoring is active prior to start of service.
- Coordinate with the Customer to maintain Motorola service authentication credentials.
- Monitor the Customer’s ASTRO 25 network and applicable CEN systems 24/7 for malicious or unusual activity, using trained and accredited technicians.

- Respond to security incidents in the Customer's system in accordance with Section 1.4.1.1.2 Managed Detection and Response Elements. Response may include, but is not limited to, requesting additional information from the Customer, continuing to monitor the event for further development or informing the Customer to enact the Customer's documented Incident Response plan.
- Assist the Customer with identifying devices that support logging within the ASTRO 25 network and applicable CEN systems have been configured to forward Syslog events to the AERSS.
- Provide the Customer with access to the ActiveEye platform enabling Customer access to security event and incident details.

Customer Responsibilities

- The ASTRO 25 MDR service requires a connection from the Customer's ASTRO 25 network and applicable CEN systems to the Internet. Establish connectivity with sufficient bandwidth before the service commences. Internet service bandwidth requirements are as follows:
  - Bandwidth throughput 10 Mbps per AERSS.
  - High availability Internet Connection (99.99% (4-9s) or higher).
  - Packet loss < 0.5%.
  - Jitter <10 ms.
  - Delay < 120 ms.
  - RJ45 Port Speed - Auto Negotiate.
  - If an ASTRO site link will be leveraged for endpoint detection and response communications, that site link must support a minimum of 2 Mbps of bandwidth.
- It is the Customer's responsibility or the contracted maintainer to install the AERSS device in the Control Room CEN.
- Allow Motorola continuous remote access to monitor the ASTRO 25 network and applicable CEN systems. This includes keeping the connection active, providing passwords, and working with Motorola to understand and maintain administration privileges.
- Maintain an active subscription for:
  - Security Update Service (SUS) (or Remote Security Update Service), ensuring patches and antivirus definitions are applied according to the release cadence of the service.
  - ASTRO Dispatch Service and ASTRO Infrastructure Response.
- Provide continuous utility services to any equipment installed or utilized at the Customer's premises to support service delivery and remote monitoring.
- Provide Motorola with contact information necessary to complete the Customer Support Plan (CSP). Notify the Customer's System Manager (SM) within two weeks of any contact information changes.
- Notify Motorola if any components are added to or removed from the environment as it may be necessary to update or incorporate in MDR. Changes to monitored components may result in changes to the pricing of the MDR service.
- **Ensure that the ASTRO 25 system is operating on a Motorola supported release.**
- Allow Motorola dispatched field service technicians physical access to monitoring hardware when required.

- Cooperate with Motorola and perform all acts that are required to enable Motorola to provide the services described in this SOW.
- Configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a ports on a switch) network traffic to the ActiveEye sensor for applicable CEN systems.
- Responding to Cybersecurity Incident Cases created by the Motorola SOC.

1.4.1.1.5 Service Modules

Log Collection / Analytics

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

Motorola Responsibilities

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

Customer Responsibilities

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

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

Network Detection

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

Motorola Responsibilities

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

Customer Responsibilities

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

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

Endpoint Detection and Response

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

Motorola Solutions Responsibilities

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

Customer Responsibilities

- Work with Motorola to ensure that there is a documented incident response plan that indicates how Motorola should engage with the Customer in the event of a detection of an indicator of compromise.
- Provide and maintain contact information for a Customer point of contact that can take action or authorize Motorola to take action in the event of a detection of an indicator of compromise.

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

External Vulnerability Scanning

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

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

Motorola Responsibilities

- Configure scans to match the Customer's preferences for external scope.
- Verify vulnerability scans are operating correctly.

- Make generated results available in the Customer's ActiveEye portal.
- Create ticket notifications for significant, new findings of interest.

Customer Responsibilities

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

Applies to Internet facing assets only.

1.4.1.1.6 Security Operations Center Monitoring and Support

Scope

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

Motorola's SOC is staffed with security experts who will use ActiveEye security platform to monitor elements integrated by service modules. In addition, SOC staff will take advantage of their extensive experience to investigate and triage detected threats, and to recommend responses to the Customer. Depending on Customer security policies and the extent to which endpoint detection and response is deployed within the system, the SOC may take actions to deploy countermeasures in an attempt to contain a security incident. Customer support is provided in the English language.

Motorola will start monitoring the ASTRO 25 MDR service in accordance with Motorola processes and procedures after deployment, as described in Section 1.4.1.1.3 Deployment Timeline and Milestones.

The SOC receives system-generated alerts 24/7, and provides the Customer with a toll-free telephone number and email address for support requests, available 24/7. Support requests are stored in a ticketing system for accountability and reporting. The SOC will respond to detected events in accordance with Section 1.4.1.1.7 Incident Priority Level Definitions and Response Times.

Ongoing Security Operations Center Service Responsibilities

Motorola Responsibilities

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

- Engage the Customer's defined Incident Response Process.

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

Customer Responsibilities

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

Technical Support

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

Motorola Responsibilities

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

Customer Responsibilities

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

Limitations and Exclusions

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

Incident Response

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

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

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

Motorola Responsibilities

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

Customer Responsibilities

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

Event Response and Notification

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

Table 1-1: Event Handling

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

Notification

Motorola 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 (EOI). These can be formatted for automated processing, e.g., by ticketing systems.
Urgent Notification Procedure	Additional, optional means and addresses for notifications of Events of Interest that require urgent notification. These usually include telephone notifications.

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

Tuning

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

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

Tuning Period Exception

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

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

1.4.1.1.7 Incident Priority Level Definitions and Response Times

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

Priority	Definition	Service Coverage
Critical	Security incidents that have caused, or are suspected to have caused significant damage to the functionality of the Customer's ASTRO 25 system or information stored within it. Efforts to recover from the incident may be significant. Examples: ▪ Malware that is not quarantined by anti-virus. ▪ Evidence that a monitored component has communicated with suspected malicious actors.	Response provided 24 hours, 7 days a week, including United States (U.S.) public holidays.

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

Response Time Goals

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

ActiveEye Platform Availability

The platform utilizes a multi-zone architecture which can recover from failures in different data collection, enhancement, analysis, and visualization tiers. Motorola will make commercially reasonable

efforts to provide monthly availability of 99.9% for the ActiveEye Platform services. Service availability is subject to limited scheduled downtime for servicing and upgrades, as well as unscheduled and unanticipated downtime resulting from circumstances or events outside of Motorola's reasonable control, such as disruptions of, or damage, to the Customer's or a third-party's information or communications systems or equipment, telecommunication circuit availability/performance between Customer sites, any on-premises core and/or between on-premises equipment and the ActiveEye Platform.

ActiveEye Remote Security Sensor (AERSS)

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

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

1.4.1.1.8 Included Services

Site Information

The following quantities are included in the scope:

Site / Location	Quantity
Primary zone cores	1
DSR backup cores	0
Sites (NMD, T-Sub, C-Sub)	2
CEN (Control Room)	0
CEN (RNI-DMZ)	1
Network Management Clients	3
Dispatch Consoles	25
AIS	2
CEN Endpoints	20

Services Included

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

Service Module	Features Included	Network Environment	Subscribed
ActiveEye Remote Security Sensor (AERSS)	Number of sensors:		Yes

Service Module	Features Included	Network Environment	Subscribed
Log Collection / Analytics	Online Storage: 30 days Extended Log Storage: 12 Months		Yes
Network Detection	Up to 1 Gbps per sensor port		Yes
Endpoint Detection and Response	Cortex XDR		Yes
External Vulnerability Scanning			Yes/No

The following table lists any ancillary components required.

1.4.1.1.9 Limitations and Exclusions

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

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

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

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

Service Limitations

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

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

Customer understands and agrees that data obtained, accessed, or utilized in the performance of the services may be transmitted to, accessed, monitored, and/or otherwise processed by Motorola in the

U.S. and/or other Motorola operations globally. Customer consents to and authorizes all such processing and agrees to provide, obtain, or post any necessary approvals, consents, or notices that may be necessary to comply with applicable law.

Customer and Third-Party Information

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

Third-Party Software and Service Providers, Including Resale

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

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

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

1.4.1.2 Network Event Monitoring

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

1.4.1.2.1 Description of Service

With Network Event Monitoring, Motorola uses a Managed Services Suite of Tools (MSST) to detect events 24/7 as they occur, analyze them, and escalate them to the Network Operation Center (NOC). Incidents will be generated automatically based on the criteria shown in Table 1-3: Alarm Threshold Rule Options for all Event Types.

Table 1-3: Alarm Threshold Rule Options for all Event Types

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

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

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

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

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

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

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

1.4.1.2.2 Scope

Network Event Monitoring is available 24/7. Incidents generated by the monitoring service will be handled in accordance with Section 1.9 Priority Level Definitions and Response Times.

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

1.4.1.2.3 Inclusions

Network Event Monitoring is available for the devices listed in Section 1.4.1.2.6: Monitored Elements.

Motorola Responsibilities

- Provide a dedicated network connection necessary for monitoring the Customer's communication network. Section 1.4.1.2.4 Connectivity describes available connectivity options.
- If determined necessary by Motorola Solutions, provide Motorola Solutions-owned equipment at the Customer's premises for monitoring network elements. The type of equipment and location of deployment is listed in Section 1.4.1.2.5 Motorola Owned and Supplied Equipment.
- Verify connectivity and event monitoring prior to system acceptance or start date.
- Monitor system continuously during hours designated in the Customer Support Plan (CSP), and in accordance with Section 1.9 Priority Level Definitions and Response Times.
- Remotely access the Customer's system to perform remote diagnosis as permitted by the Customer pursuant to Section 1.4.1.2.3 Customer Responsibilities below.
- Create an incident, as necessary. Gather information to perform the following:
  - Characterize the issue
  - Determine a plan of action
  - Assign and track the incident to resolution
- Provide the Customer with system configuration info, site info, system notifications, and system notes via Customer Hub.
- Cooperate with the Customer to coordinate the transition of monitoring responsibilities between Motorola Solutions and the Customer as specified in Section 1.4.1.2.3 Customer Responsibilities below.
- Maintain communication as needed with the Customer in the field until incident resolution.
- Provide available information on incident resolution to the Customer.

Limitations and Exclusions

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

- Motorola will not monitor any elements outside of the Customer's ASTRO 25 network, or monitor infrastructure provided by a third-party, unless specifically stated. Monitored elements must be within the ASTRO 25 radio network and capable of sending alerts to the Unified Event Manager (UEM).
- Additional support charges above contracted service agreement fees may apply if Motorola determines that system faults were caused by the Customer making changes to critical system parameters without written agreement from Motorola.
- Monitoring of network transport, such as WAN ports, WAN cloud, and redundant paths, unless provided by supplemental service outside this standard scope.
- Elements deployed outside of ASTRO RNI (E.g.: ASTRO CEN sites) are excluded from the service.

- Emergency on-site visits required to resolve technical issues that cannot be resolved by working remotely with the Customer's technical resource.
- System installations, upgrades, and expansions.
- Customer training.
- Hardware repair and/or replacement.
- Network security services.
- Information Assurance.

Customer Responsibilities

- Allow Motorola Solutions continuous remote access to enable the monitoring service.
- Provide continuous utility service to any Motorola Solutions equipment installed or used at the Customer's premises to support delivery of the service. The Customer agrees to take reasonable due care to secure the Motorola Solutions equipment from theft or damage while on the Customer's premises.
- Prior to contract start date, provide Motorola Solutions with pre-defined information necessary to complete a CSP, including:
  - Incident notification preferences and procedure.
  - Repair verification preference and procedure.
  - Database and escalation procedure forms.
- Submit timely changes in any information supplied to Motorola Solutions and included in the CSP to the System Manager (SM).
- Notify the CMSO when the Customer performs any activity that impacts the system. Activity that impacts the system may include, but is not limited to: installing software or hardware upgrades, performing upgrades to the network, renaming elements or devices within the network, and taking down part of the system to perform maintenance.
- Send system configuration change requests to Motorola Solutions' SM via Customer Hub.
- Allow Motorola Solutions' field service technician, if designated in the CSP, access to equipment, including any connectivity or monitoring equipment, if remote service is not possible.
- Allow Motorola Solutions' field service technician, if designated in the CSP, access to remove Motorola Solutions-owned monitoring equipment upon cancellation of service.
- Provide Motorola Solutions with all Customer-managed passwords required to access the Customer's system upon request, when opening a request for service support, or when needed to enable response to a technical issue.
- Pay additional support charges above the contracted service agreements that may apply if it is determined that system faults were caused by the Customer making changes to critical system parameters without written agreement from Motorola Solutions.
- In the event that Motorola Solutions agrees in writing to provide supplemental monitoring for third-party elements provided by the Customer, the Customer agrees to obtain third party consents or licenses required to enable Motorola Solutions to provide the monitoring service.
- Cooperate with Motorola Solutions and perform reasonable or necessary acts to enable Motorola Solutions to provide these services.

- Contact Motorola Solutions to coordinate transition of monitoring when the responsibility for monitoring needs to be transferred to or from Motorola Solutions, as specified in pre-defined information provided in the Customer's CSP. An example of a transfer scenario is transferring monitoring from Motorola Solutions for network monitoring after normal business hours.
  - Upon contact, the Customer must provide Motorola Solutions with customer name, site ID, status on any open incidents, priority level of any open incidents, brief descriptions of any ongoing incident, and action plan for resolving those incidents.
- Acknowledge that incidents will be handled in accordance Section 1.9 Priority Level Definitions and Response Times.

1.4.1.2.4 Connectivity

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

Table 1-4: Available Connectivity

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

1.4.1.2.5 Motorola Owned and Supplied Equipment

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

Table 1-5: Motorola Owned and Supplied Equipment

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

1.4.1.2.6 Monitored Elements

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

Table 1-6: Monitored Elements

Monitored Elements		
Active Directory	Enrichment Testing	Probe
Agent	Environmental	Core Switch
AIS	ESX	Radio Interface
AMB	Exit Router	RDM
Application Server	RNI Firewall	RFDS
APX Cloud Application	Core Server	RGU
ATR	Gateway	RNG

Monitored Elements		
AUC	Gateway Router	Site Router
Backup Server	Gateway Unit	RTU
Base Radio	GIS Server	SCOM Server
Call Processor	HSS	Short Data Router
Camera	Install Server	Statistical Server
CBSD	Site Switch	Storage Networking
CCGW	Licensing Service	Consoles
Channel	Load Balancer	TRAK
Client Station	Logging Recorder	Terminal Server
CommandCentral AXS dispatch console	Logging Replay Station	Time Keeper
Controller	UNC	Training App
Conventional	UEM	Training Database
Core Router	MOSCAD Server	Trap Forwarder
Data Processing	Network Address	UCS
Database Server	Network Device	Licensing Server
Data Warehouse Server	NTP	Virtual Machine
Device Configuration Server	AIS	VMS
DNS	Application Server	VPM
Domain Controller	Packet Data Gateway	WSGU
D series Site Controller	Physical Host Environmental	ZDS
eNodeB	Physical Host Power and Network	Zone Controller
Active directory	Power Distribution Unit	Syslog
Repeaters	Power Monitor	Proxy

1.4.1.3 ASTRO Connectivity Services

To establish a connection between the Customer's on-premises ASTRO 25 infrastructure core and Motorola Solutions Network and Security Operation Centers, Motorola will provide required network equipment with sufficient bandwidth as mentioned in Section 1.4.1.2.5: Motorola Owned and Supplied Equipment. The connectivity to customer’s ASTRO 25 infrastructure core will terminate upon the Customer canceling their ASTRO 25 service package.

Motorola Responsibilities

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

- Perform a site survey prior to installation to assess that all the conditions for a proper site installation can be met, including, but not limited to the presence of network facilities necessary to provide the necessary connectivity.

- Motorola will note any variations of the site that would affect the hardware specifications or estimated labor involved for a standard installation. If the site survey indicates a non-standard installation (for example, the need for construction of “last mile” network facilities), then a mutually agreed change order may be required.
- It is assumed that in the building, LTE coverage is adequate at the installation site. If, during installation, it is determined the in-building LTE coverage is not adequate for service, then a mutually agreed change order may be required for external antenna installation.
- Standard Demarc – Motorola will install cable between the Local Exchange Carrier Minimum Point of Entry (MPOE) and the Managed Elements located within the customer ASTRO infrastructure. Motorola will install the demarc standard – which includes one service call, up to two (2) total hours of on-site labor, and installation of one (1) cat 3, 5, or 5e cable drop up to 150-feet (vertical length up to 12-feet), connectors, ty-wraps, jacks, face plates, and cable. A mutually agreed change order may be required if the site survey indicates a non-standard extended demarc (for example, the need for cable through walls over 150-feet or multiple floors).
- Install equipment supplied by Motorola. Installation period is estimated to be within 45 business days from when Motorola and Customer execute the Agreement and related addendum or addenda.
- Cooperate with the Customer to schedule the ASTRO 25 Connectivity Service implementation.
- Administer safe work procedures for installation of the remote access circuit.

Customer Responsibilities

- Sign the Transport Connectivity Addendum (TCA).
- Provide space for the networking equipment at the core site.
- Ensure communications sites meet space, grounding, power, and connectivity requirements for equipment installation.
- Obtain all licensing, site access, or permitting required for project implementation.
- Provide a dedicated delivery point (such as a warehouse), for receipt, inventory, and storage of equipment prior to delivery to the site(s), if requested by Motorola.
- Ensure existing sites or equipment locations have sufficient space available for the system, as specified by Motorola's R56 Standards and Guidelines for Communication.
- Ensure that existing sites or equipment locations have adequate electrical power in the proper phase, in the proper voltage, and with necessary site grounding to support the requirements of the equipment provided with the ASTRO 25 Connectivity Service.
- Perform any location upgrades or modifications.
- Obtain and maintain approved local, State, or Federal permits necessary for installing and operating the proposed equipment.
- Provide any required system interconnections not specifically included in the ASTRO 25 Connectivity Service.
- Install demarcation equipment, air conditioning, and other equipment that is not provided by Motorola and is necessary to support the project.
- Perform work necessary to complete the connectivity provisioning outside the scope of the installation provided by Motorola.

- If Motorola's design requires wireless backup and out-of-band (OOB) monitoring, Motorola may provide a wireless modem at the Customer location for OOB monitoring for Motorola Solutions Monitored Elements. The Customer shall provide access and accommodations to install the modem if required.
- The Customer will notify Motorola of any maintenance that may affect the operating status of the service using a Customer Maintenance Change Management Request via the Customer Hub. Examples of maintenance activities include: powering down the site, a Motorola Managed Element, or a third-party Network Terminating Unit; or, resetting, recabling, or moving equipment components.
- If a Motorola representative visits the Customer Site or works remotely, at the Customer's request, to investigate an issue with the Service, and the Motorola representative determines the Service is functioning correctly or is prevented from resolving the issue because the Customer did not provide access or reasonable assistance, the Customer will be charged at published or negotiated time and material rates.
- Upon termination of the services, Customer shall promptly return to Motorola all equipment provided by Motorola in conjunction with the ASTRO 25 Connectivity Service and not explicitly owned by Customer. Motorola is entitled to invoice any and all costs arising out of or in connection with Customer's failure to return the Motorola equipment if the Motorola equipment is not returned within sixty (60) days following termination of services.

Limitations/Exclusions

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

1.4.1.4 Remote Technical Support

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

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

1.4.1.4.1 Description of Service

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

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

The CMSO Operations Center classifies and responds to each technical support request in accordance with 1.8: Priority Level Definitions and Response Times.

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

1.4.1.4.2 Scope

The CMSO Service Desk is available via telephone 24/7 to receive and log requests for technical support. Remote Technical Support service is provided in accordance with Section 1.9 Priority Level Definitions and Response Times.

1.4.1.4.3 Inclusions

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

Motorola Responsibilities

- Maintain availability of the Motorola CMSO Service Desk via telephone (800-MSI-HELP) 24/7 to receive, log, and classify Customer requests for support.
- Respond to incidents and technical service requests in accordance with 1.8: Priority Level Definitions and Response Times.
- Provide caller a plan of action outlining additional requirements, activities, or information required to achieve restoral/fulfillment.
- Maintain communication with the Customer in the field as needed until resolution of the incident.
- Coordinate technical resolutions with agreed upon third-party vendors, as needed.
- Escalate support issues to additional Motorola technical resources, as applicable.
- Determine, in its sole discretion, when an incident requires more than the Remote Technical Support services described in this SOW and notify the Customer of an alternative course of action.

Limitations and Exclusions

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

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

Customer Responsibilities

- Prior to contract start date, provide Motorola with pre-defined information necessary to complete CSP.
- Submit timely changes in any information supplied in the CSP to the SM.

- Contact the CMSO Service Desk to engage the Remote Technical Support service when needed, providing the necessary information for proper entitlement services. This information includes, but is not limited to, the name of contact, name of Customer, system ID number, site(s) in question, and a brief description of the problem that contains pertinent information for initial issue classification.
- Maintain suitably trained technical resources familiar with the operation of the Customer's system to provide field maintenance and technical maintenance services for the system.
- Supply suitably skilled and trained on-site presence when requested.
- Validate issue resolution in a timely manner prior to close of the incident.
- Acknowledge that incidents will be addressed in accordance with Section 1.9 Priority Level Definitions and Response Times
- Cooperate with Motorola, and perform all acts that are reasonable or necessary to enable Motorola to provide Remote Technical Support.
- In the event that Motorola agrees in writing to provide supplemental Remote Technical Support to third-party elements provided by the Customer, the Customer agrees to obtain all third-party consents or licenses required to enable Motorola to provide the service.

1.4.1.5 Network Hardware Repair with Advanced Replacement

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

1.4.1.5.1 Description of Service

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

Network Hardware Repair is also known as Infrastructure Repair.

1.4.1.5.2 Scope

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

1.4.1.5.3 Inclusions

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

Motorola Responsibilities

- Provide the Customer access to the CMSO Service Desk, operational 24/7, to request repair service.
- Provide repair return authorization numbers when requested by the Customer.

- Receive malfunctioning infrastructure components from the Customer and document its arrival, repair, and return.
- Conduct the following services for Motorola infrastructure:
  - Perform an operational check on infrastructure components to determine the nature of the problem.
  - Replace malfunctioning components.
  - Verify that Motorola infrastructure components are returned to applicable Motorola factory specifications.
  - Perform a box unit test on serviced infrastructure components.
  - Perform a system test on select infrastructure components.
- Conduct the following services for select third-party infrastructure:
  - When applicable, perform pre-diagnostic and repair services to confirm infrastructure component malfunctions and prevent sending infrastructure components with No Trouble Found (NTF) to third-party vendor for repair.
  - When applicable, ship malfunctioning infrastructure components to the original equipment manufacturer or third-party vendor for repair service.
  - Track infrastructure components sent to the original equipment manufacturer or third-party vendor for service.
  - When applicable, perform a post-test after repair by original equipment manufacturer or third-party vendor to confirm malfunctioning infrastructure components have been repaired and function properly in a Motorola system configuration.
- Reprogram repaired infrastructure components to original operating parameters based on software and firmware provided by the Customer, as required in Section 1.4.1.5.3 Customer Responsibilities. If the Customer's software version and configuration are not provided, shipping will be delayed. If the repair depot determines that infrastructure components are malfunctioning due to a software defect, the repair depot reserves the right to reload these components with a different but equivalent software version.
- Properly package repaired infrastructure components.
- Ship repaired infrastructure components to Customer-specified address during normal operating hours of Monday through Friday from 7:00 a.m. to 7:00 p.m. Central Standard Time (CST), excluding holidays. Infrastructure component will be sent using two-day air shipping unless the Customer requests otherwise. Motorola will pay for shipping unless the Customer requests shipments outside of the above mentioned standard business hours or carrier programs, such as next flight out (NFO). In such cases, the Customer will be responsible for paying shipping and handling charges.

Limitations and Exclusions

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

- All Motorola radio infrastructure components over the post-cancellation support period.
- All third-party radio infrastructure components over the post-cancellation support period.
- All broadband infrastructure components over the post-cancellation support period.
- Physically damaged infrastructure components.

- Third-party equipment not shipped by Motorola.
- Consumable items including, but not limited to, batteries, connectors, cables, toner or ink cartridges, tower lighting, laptop computers, monitors, keyboards, and mouse.
- Video retrieval from digital in-car video equipment.
- RF infrastructure and backhaul components, including but not limited to, antennas, transmission lines, antenna dehydrators, microwave, line boosters, amplifiers (such as tower top amplifiers and bi-directional amplifiers), logging recorders, data talker wireless transmitters, short haul modems, combiners, multicouplers, duplexers, shelters, shelter HVAC, generators, UPS's, dropship nonstandard items and test equipment ***except as specifically described in this proposal***.
- Racks, furniture, and cabinets.
- Non-standard configurations, customer-modified infrastructure, and certain third-party dropship products.
- Firmware or software upgrades.

Customer Responsibilities

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

1.4.1.5.4 Repair Process

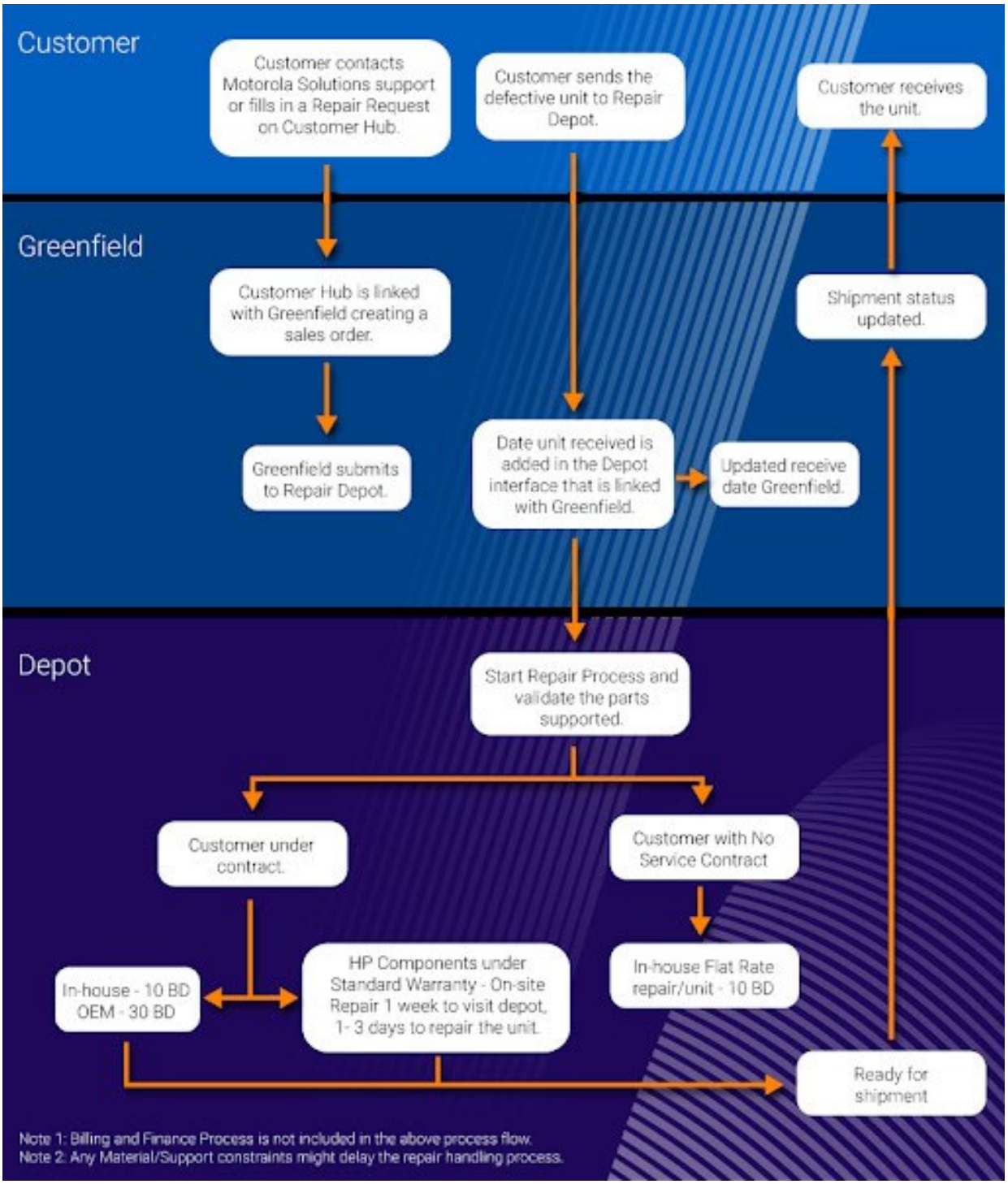


Figure 1-1: Repair Decision Process

1.4.1.5.5 Advanced Replacement

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

Customers who prefer to maintain their own FRU inventory may request an FRU while their unit is being repaired. Refer to Figure 1-2: Advanced Replacement Decision Process for details on the unit loan process.

Added Motorola Responsibilities for Advanced Replacement

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

Added Customer Responsibilities for Advanced Replacement

- Pay for Advanced Replacement FRU shipping from Motorola repair depot if the Customer requested shipping outside of standard business hours or carrier programs set forth in Section 4.1.5.5: Added Motorola Responsibilities for Advanced Replacement. See Table 1-7: Shipping Charges and Default Mail Service for shipping charge details.

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

1.4.1.5.6 Replacement Process for Advanced Replacement

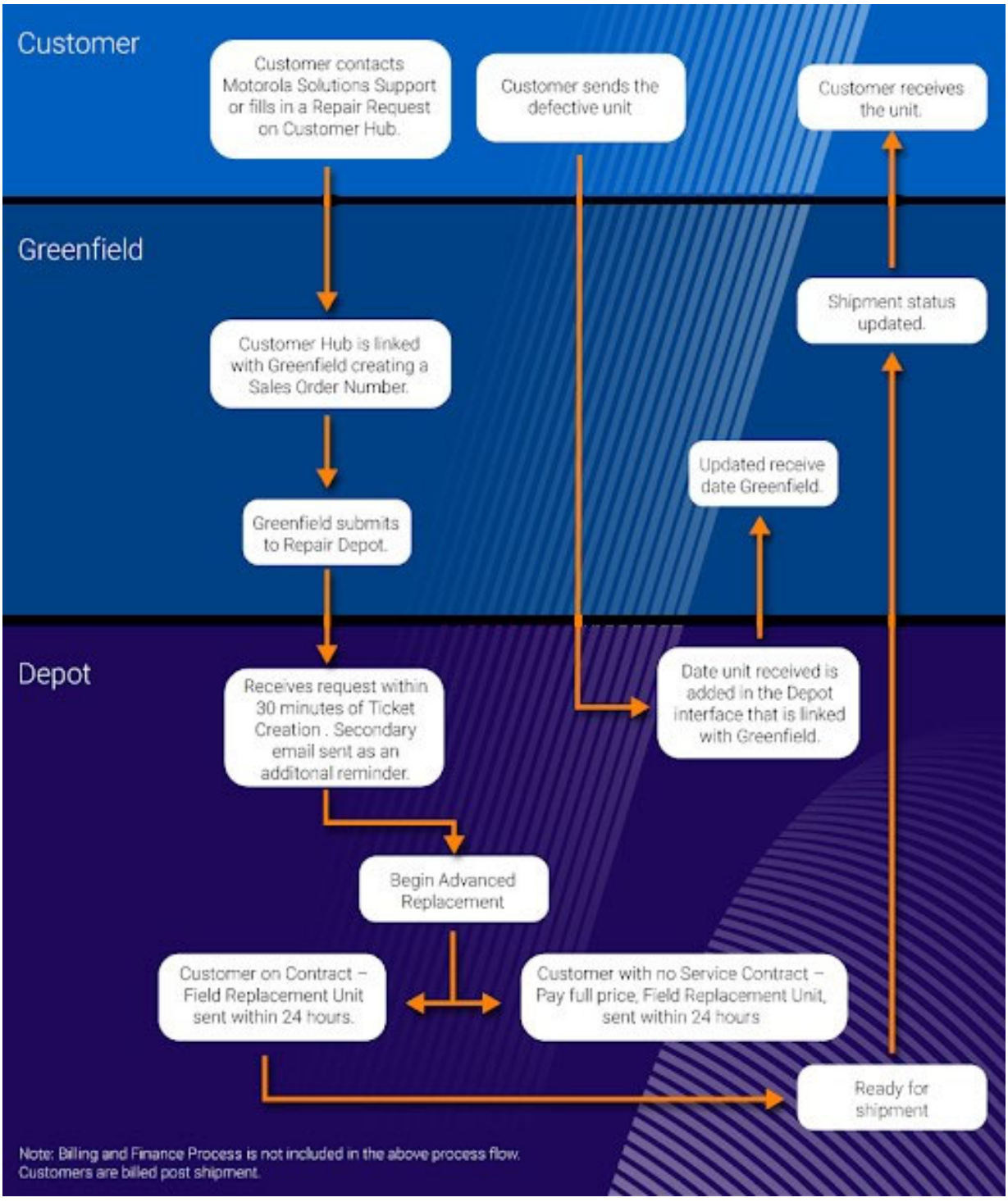


Figure 1-2: Advanced Replacement Decision Process

Table 1-7: Shipping Charges and Default Mail Service

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

Motorola shipping carrier – FedEx.

1.4.1.6 Security Update Service

Motorola's ASTRO 25 Security Update Service (SUS) provides pretested security updates, minimizing cyber risk and software conflicts. These security updates contain operating system security patches and antivirus definitions that have been validated for compatibility with ASTRO 25 systems. Security update delivery is determined by the options included as part of this service. Section 1.4.1.6.4: Inclusions indicates if options are included as part of this service.

1.4.1.6.1 Description of Service

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

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

Note, the ASTRO 25 Advanced Plus Service also includes the Remote Security Update Service. See Section 1.4.1.7. Customer download and self-installation of security updates is only necessary for the system components that are not covered by RSUS. See Section 1.10 Appendix 1 for RSUS scope and exclusions.

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

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

1.4.1.6.2 On-Site Delivery

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

1.4.1.6.3 Scope

RSUS includes pretested security updates for the software listed in Table 1-8: Update Cadence. This table also describes the release cadence for security updates.

Table 1-8: Update Cadence

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

1.4.1.6.4 Inclusions

Supported ASTRO 25 core types and security update delivery methods are included in Table 1-9: SUS Packages. This table indicates if Motorola will provide any SUS optional services to the Customer. SUS supports the current Motorola ASTRO 25 system release and aligns with the established Software Support Policy (SwSP).

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

Table 1-9: SUS Packages

Service	ASTRO 25 Core Type	Included
Security Update Service Customer Self-installed	L Core M Core Simplified Core	X

Service	ASTRO 25 Core Type	Included
Security Update Service with Reboot Support	L Core M Core Simplified Core	
Security Update Service with On-Site Delivery	L Core M Core Simplified Core	

Responsibilities for downloading and installing security updates and rebooting applicable hardware are detailed in Section 1.4.1.6.5: Installation and Reboot Responsibilities.

Motorola Responsibilities

- On the release schedule in Section 1.4.1.6.3: Scope review relevant and appropriate security patches released by Original Equipment Manufacturer (OEM) vendors.
- Release tested and verified security patches to Motorola's secure website.
- Publish documentation for installation, recommended configuration changes, any identified issue(s), and remediation instructions for each security update release.
- Send notifications by email when security updates are available to download from the secure website.

Limitations and Exclusions

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

Customer Responsibilities

- Provide Motorola with predefined information necessary to complete a Customer Support Plan (CSP) prior to the Agreement start date.

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

1.4.1.6.5 Installation and Reboot Responsibilities

Installation and Reboot responsibilities are determined by the specific SUS package being purchased. Table 1-10: Installation and Reboot Responsibilities Matrix contains the breakdown of responsibilities. Section 1.4.1.6.4: Inclusions indicates which services are included.

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

Table 1-10: Installation and Reboot Responsibilities Matrix

SUS Package	Motorola Responsibilities	Customer Responsibilities
Security Update Service Customer Self-installed		▪ Deploy pretested files to the Customer's system as instructed in the "Read Me" text provided on Motorola's secure website. ▪ 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. ▪ When a security update requires a reboot, reboot servers and workstations after security updates are installed.	▪ Acknowledge Motorola will reboot servers and workstations, and agree to timing.

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

Disclaimer

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

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

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

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

1.4.1.7 Remote Security Update Service

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

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

1.4.1.7.1 Description of Service

Motorola remotely installs pretested security updates on the applicable ASTRO 25 system components, as defined in Section 1.10 Appendix 1.

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

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

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

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

Application of Prerequisite Motorola Technical Notices (MTN)

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

Updates to System Components in the Customer Enterprise Network

Connections to other networks, herein referred to as Customer Enterprise Network (CEN), are delineated by firewalls. All security updates deployed by RSUS are specific to the equipment included in the ASTRO 25 radio network. The only exceptions are those identified as RSUS exceptions in Section 1.10 Appendix 1.

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

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

Microsoft Windows Reboot Following Security Update Installation

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

Failure of the Customer to fulfill reboot responsibilities as described in Table 1-13: Reboot Responsibilities Matrix exposes systems to security threats. Until reboot, the system is not updated.

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

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

Reboot Support

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

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

- This process is repeated monthly.

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

1.4.1.7.2 Scope

RSUS includes pretested security updates for the software listed in Table 1-11: Update Cadence. This table also describes the release cadence for security updates.

Table 1-11: Update Cadence

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

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

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

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

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

Intrusive security updates require Customer coordination, may require hardware reboots and zone controller rolling (switching from one zone controller to the other) to fully implement. Systems with redundant zone controllers (M3) have low downtime (minutes) as the zone controllers are rolled but systems with single zone controllers will be down for longer periods. While rolling the zone controllers, the system will operate in “site trunking” mode. The Customer will need to be aware of these operational impacts, and coordinate events with users.

1.4.1.7.3 Tenanted Customers Access to Antivirus Updates

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

1.4.1.7.4 Inclusions

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

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

Table 1-12: RSUS Options

Service	ASTRO 25 Core Type	Included
Remote Security Update Service	L Core M Core Simplified Core	X
Remote Security Update Service with Reboot Support	L Core M Core Simplified Core	

Responsibilities for rebooting applicable hardware are detailed in Section 1.4.1.7.5: Reboot Responsibilities.

Motorola Responsibilities

- Remotely deploy patches listed in Section 1.4.1.8.2: Scope on the Customer's system. Patches will be installed on the cadence described in that section.
  - As outlined in Section 1.4.1.8.2: Scope, coordinate and communicate with the Customer when installing updates that will require server reboots, workstation reboots, or both.
  - Install non-intrusive updates, like antivirus definitions, as released without coordination.
- In the event that no security updates are released by the Original Equipment Manufacturers (OEM), the Final RSUS Patch Report can be reviewed by the Customer to identify where no new security updates were required.
- Coordinate RSUS activities with any other Motorola system maintenance or other engineering activities with the Customer to minimize downtime, inefficiency and operational impact.

Limitations and Exclusions

- Systems with non-standard configurations that have not been certified by Motorola's Systems Integration and Test (SIT) team are specifically excluded from this service, unless otherwise agreed in writing by Motorola.
- Interim or unplanned releases outside the supported release cadence.
- Service does not include pretested intrusion detection system (IDS) signature updates for IDS solutions.
- This service does not include releases for Motorola products that are not ASTRO 25 L, M, and Simplified Core radio network infrastructure equipment. The following are examples of excluded products: WAVE PTX, Critical Connect, and VESTA solutions.

- K Core ASTRO 25 systems are excluded.
- Motorola product updates are not included in these services.
- Shared network infrastructure firmware, such as transport and firewall firmware are not included in these services.
- This service excludes the delivery of MTNs to the customer system.
- Motorola does not represent that it will identify, fully recognize, discover, or resolve all security events or threats, system vulnerabilities, malicious codes or data, backdoors, or other system threats or incompatibilities as part of the service, or that the agreed upon cadence/time of delivery will be sufficient to identify, mitigate or prevent any cyber incident.
- Motorola shall provide Customers with a list of MTNs that are prerequisite for execution of the RSUS service.

Customer Responsibilities

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

1.4.1.7.5 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 1-13: Reboot Responsibilities Matrix contains the breakdown of responsibilities. Section 1.4.1.8.4: Inclusions indicates which services are included.

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

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

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

Table 1-13: Reboot Responsibilities Matrix

Remote SUS Package	Motorola 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. ▪ When remote deployment is in progress, it may be necessary for multiple reboots to be coordinated with Motorola.
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.	

Disclaimer

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

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

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

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

1.4.1.8 Motorola Standard On-Site Infrastructure Response

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

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

1.4.1.8.1 Description of Service

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

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

The dispatched field service technician will travel to the Customer's location to restore the system in accordance with Section 1.4.1.8.5: Priority Level Definitions and Response Times.

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

1.4.1.8.2 Scope

On-Site Infrastructure Response is available in accordance with Section 1.4.1.8.5: Priority Level Definitions and Response Times. Customer's Response Time Classification is designated in the Customer Support Plan.

1.4.1.8.3 Geographical Availability

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

1.4.1.8.4 Inclusions

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

Motorola Responsibilities

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

  - Open, assigned to the Motorola field service technician, arrival of the field service technician on-site, delayed, or closed.
- Provide incident activity reports to the Customer, if requested.

Limitations and Exclusions

The following items are excluded from this service:

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

Customer Responsibilities

- Contact Motorola, as necessary, to request service.
- Prior to start date, provide Motorola with the following pre-defined Customer information and preferences necessary to complete CSP:
  - Incident notification preferences and procedure.
  - Repair verification preference and procedure.
  - Database and escalation procedure forms.
- Submit timely changes in any information supplied in the CSP to the SM.
- Provide the following information when initiating a service request:
  - Assigned system ID number.
  - Problem description and site location.
  - Other pertinent information requested by Motorola to open an incident.
- Provide field service technician with access to equipment.
- Supply infrastructure spare or FRU, as applicable, in order for Motorola to restore the system.
- Maintain and store software needed to restore the system in an easily accessible location.

- Maintain and store proper system backups in an easily accessible location.
- If required by repair verification preference provided by the Customer, verify with the CMSO Service Desk and dispatch that restoration is complete or system is functional.
- Cooperate with Motorola and perform reasonable or necessary acts to enable Motorola to provide these services.
- In the event that Motorola agrees in writing to provide supplemental On-Site Infrastructure Response to Customer-provided third-party elements, the Customer agrees to obtain and provide applicable third-party consents or licenses to enable Motorola to provide the service.

1.4.1.8.5 Priority Level Definitions and Response Times

This section describes the criteria Motorola used to prioritize incidents and service requests, and lists the response times for those priority levels. Motorola's proposal includes Standard On Site Response.

Table 1-14: Proposed - Standard Level Definitions and Response Times

Incident Priority	Incident Definition	On-Site Response Time
Critical P1	**Core**: Core server or core link failure. No redundant server or link available. **Sites/Subsites**: Primary site down. Two RF sites or more than 10% of RF sites down, whichever is greater. **Consoles**: More than 40% of a site's console positions down. **Conventional Channels**: Conventional Channel Gateways (CCGW) down without redundant gateways available. **Security Features**: Security is non-functional or degraded.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
High P2	**Core**: Core server or link failures. Redundant server or link available. **Consoles**: Between 20% and 40% of a site's console positions down. **Sites/Subsites**: One RF site or up to 10% of RF sites down, whichever is greater. **Conventional Channels**: Up to 50% of CCGWs down. Redundant gateways available. **Network Elements**: Site router, site switch, or GPS server down. No redundant networking element available.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
Medium P3	**Consoles**: Up to 20% of a site's console positions down. **Conventional Channels:** Single channel down. Redundant gateway available. **Network Elements**: Site router/switch or GPS server down. Redundant networking element available.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 8 hours of receiving dispatch notification.

Incident Priority	Incident Definition	On-Site Response Time
Low P4	**Service Requests**: Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).	Not applicable.

Table 1-15: Option - Premier Priority Level Definitions and Response Times

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

Table 1-16: Limited Priority Level Definitions and Response Times

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

1.4.1.9 Annual Preventative Maintenance

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

1.4.1.9.1 Description of Service

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

1.4.1.9.2 Scope

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

1.4.1.9.3 Inclusions

Annual Preventive Maintenance service will be delivered for Motorola-provided infrastructure, including integrated third-party products, per the level of service marked in Table 1-17: Preventive Maintenance Level.

Table 1-17: Preventive Maintenance Level

Service Level	Included
Level 1 Preventive Maintenance	X

Motorola Responsibilities

- Notify the Customer of any planned system downtime needed to perform this service.
- Maintain communication with the Customer as needed until completion of the Annual Preventive Maintenance.
- Determine, in its sole discretion, when an incident requires more than the Annual Preventive Maintenance services described in this SOW, and notify the Customer of an alternative course of action.
- Provide the Customer with a report in Customer Hub, or as otherwise agreed in the CSP, comparing system performance with expected parameters, along with any recommended actions. Time allotment for report completion is to be mutually agreed.
- Provide trained and qualified personnel with proper security clearance required to complete Annual Preventive Maintenance services.
- Field service technician will perform the following on-site:
- Perform the tasks defined in Section 1.4.1.9.4: Preventative Maintenance Tasks.
  - Perform the procedures defined in Section 1.4.1.9.5: Site Performance Evaluation Procedures for each site type on the system.
  - Provide diagnostic and test equipment necessary to perform the Preventive Maintenance service.
  - As applicable, use the Method of Procedure (MOP) defined for each task.

Limitations and Exclusions

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

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

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

Customer Responsibilities

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

1.4.1.9.4 Preventative Maintenance Tasks

The Preventive Maintenance service includes the tasks listed in this section. Tasks will be performed based on the level of service noted in Section 1.4.1.9.3: Inclusions.

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

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

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

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

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

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

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

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

RF SITE CHECKLIST – LEVEL 1	
Trunking Control Channel Redundancy	Roll control channel, test, and roll back if the site has GTR stations. This test is not applicable for D series stations.
Trunking Site Controller Redundancy, ASTRO 25 Site Repeater only	Roll site controllers with no dropped audio if the site has GTR stations. This test is not applicable for D series stations.
PM Optimization Workbook (See Section 1.4.1.9.5: Site Performance Evaluation Procedures for GTR tests)	Complete Base Station Evaluation tests - Frequency Error, Modulation Fidelity, Forward at Set Power, Reverse at Set Power, and Gen Level Desense no TX. Update station logs.

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

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

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

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

MICROWAVE CHECKLIST – LEVEL 1	
General	
Transport Connectivity	Confirm transport performance by viewing UEM for site link warnings or errors.
Backhaul Monitoring	Monitor UEM status, including alarms, logs, and events, for all links. If UEM is not used to monitor microwaves, then use an approved vendor-provided microwave alarm management server.
Radio	
Alarms	Check alarm and event history.
Software	Verify version of application.
Radio (continued)	
TX Frequency	Verify transmit frequency.
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.
Waveguide	
Visual Inspection	Inspect for wear or dents from ground using binoculars.

MICROWAVE CHECKLIST – LEVEL 1	
Connection Verification	Verify all connections are secured with proper hardware from ground using binoculars.
Dehydrator	
Visual Inspection	Inspect the 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 the structure for rust.
Cross Members	Check for damaged or missing cross members.
Safety Climb	Check safety climb for damage.
Ladder	Verify that the ladder system is secured to the 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 the paint condition.
Tower Lighting	
Lights/Markers	Verify all lights and markers are operational.
Day/Night Mode	Verify day and night mode operation.
Power Cabling	Verify that power cables are secured to the tower.
Antennas and Lines	
Antennas	Visually inspect antennas for physical damage from ground using binoculars.
Transmission Lines	Verify that all transmission lines are secure on the tower.
Grounding	
Structure Grounds	Inspect grounding for damage or corrosion
Guy Wires	
Tower Guys	Visually inspect guy wires for fraying, loss of tension, or loss of connection.
Guy Wire Hardware	Check hardware for rust.
Concrete Condition	
Tower Base	Check for chips or cracks.

1.4.1.9.5 Site Performance Evaluation Procedures

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

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)

1.4.1.10 System Upgrade Agreement (SUA)

1.4.1.10.1 Overview

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

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

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

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

1.4.1.10.2 Scope

As system releases become available, Motorola agrees to provide the Customer with the software, hardware, and implementation services required to execute up to one system infrastructure upgrade (System Upgrade) in each eligible System Upgrade window over the term of this agreement. The term of the agreement is listed in Table 1-18: SUA Terms. The eligible System Upgrade windows and their duration are illustrated in Table 1-19: Eligible Upgrade Window.

With the addition of the cloud services, Motorola will provide continuous updates to the cloud core to enable the delivery of additional functionality. Cloud updates will be more frequent than the ASTRO System Upgrades and will occur outside the defined eligible System Upgrade windows in Table 1-19: Eligible Upgrade Window. Motorola may, at its sole discretion, automatically apply the cloud updates as they become available.

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

Table 1-18: SUA Terms

Duration	8 Year(s)

Table 1-19: Eligible Upgrade Window

Eligible Upgrades	Up to one every two years

Note 1: Motorola Solutions and Fulton County shall review the "Eligible Upgrade Windows" prior to the start of each contract year.

The methodology for executing each System Upgrade is described in Section 1.4.1.10.4. ASTRO SUA pricing is based on the system configuration outlined in Section 1.6 Appendix B: System Pricing Configuration. This configuration is to be reviewed annually from the contract effective date. Any change in system configuration may require an ASTRO SUA price adjustment.

The price quoted for ASTRO SUA requires the Customer to choose a certified system upgrade path in Section 1.5 Appendix A: ASTRO 25 System Release Upgrade Paths. Should the Customer elect an upgrade path other than one listed Section 1.5 Appendix A: ASTRO 25 System Release Upgrade Paths, the Customer agrees that additional fees may be incurred to complete the implementation of the system upgrade. In this case, Motorola will provide a price quotation for any additional materials and services necessary.

1.4.1.10.3 Inclusions

Refer to Table 1-24: SUA Coverage Table for more detailed information on the SUA inclusions referenced in this section.

System Upgrades

System Upgrade coverage includes the products outlined in Appendix B: System Pricing Configuration and does not cover all products. The ASTRO SUA applies only to System Upgrades within the ASTRO platform and entitles the Customer to eligible past software versions for downgrading product software

to a compatible release version. Past versions from within the Standard Support Period will be available.

Subscriber Radio Software

The ASTRO SUA makes available the subscriber radio software releases that are shipping from the factory during the coverage period. Please refer to Section 1.4.1.10.4: General Statement of Work for System Upgrades.

Limitations and Exclusions

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

Table 1-20: SUA Limitations and Exclusions

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

Platform Migrations

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

Non-Standard Configurations

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

System Expansions and New Features

Any upgrades to hardware versions, replacement hardware, and/or implementation services that are not directly required to support the certified System Upgrade are not included unless otherwise agreed

to in writing by Motorola. This exclusion applies to, but is not limited to, system expansions and new features.

Cloud Technology

Support for Customer-provided connectivity to the cloud platform is not covered under this agreement.

Future cloud, IT, and security related adoption is an evolving technological area and laws, regulations, and standards relating to ASTRO SUA may change. Any changes to ASTRO SUA required to achieve future regulatory or Customer specific compliance requirements are not included.

Subscriber Radio Software

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

1.4.1.10.4 General Statement of Work for System Upgrades

Upgrade Planning and Preparation

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

Motorola Responsibilities

- Obtain and review infrastructure system audit data as needed.
- Identify the backlog accumulation of security patches and antivirus upgrades needed to implement a system release. If applicable, provide a quote for the necessary labor, security patches, and antivirus upgrades.
- If applicable, identify additional system hardware needed to implement a system release.
- Identify Customer provided hardware that is not covered under this agreement, or where the Customer will be responsible for implementing the system release upgrade software.
- Identify the equipment requirements and the installation plan.
- Advise the Customer of probable impact to system users during the cloud update and the actual field upgrade implementation.
- If applicable, advise the Customer on the network connection specifications necessary to perform the System Upgrade.
- Where necessary to maintain existing functionality and capabilities, deploy and configure any additional telecommunications equipment necessary for connectivity to the cloud based technologies.
- Assign program management support required to perform the certified System Upgrade. Prepare an overall System Upgrade schedule identifying key tasks and personnel resources required from Motorola and Customer for each task and phase of the System Upgrade. Conduct a review of this schedule and obtain mutual agreement of the same.
- Assign installation and engineering labor required to perform the certified System Upgrade.
- Provide access to cloud training videos, frequently asked questions, and help guide.

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

Customer Responsibilities

- Contact Motorola to schedule and engage the appropriate Motorola resources for a system Contact Motorola to schedule a System Upgrade and provide necessary information requested by Motorola to execute the System Upgrade. Review System Upgrade schedule and reach mutual agreement of the same.
- Identify hardware not purchased through Motorola that will require the system release upgrade software.
- Purchase the security patches, antivirus upgrades and the labor necessary to address any security upgrades backlog accumulation identified in Section 1.4.1.6.4: Motorola Responsibilities, if applicable. Unless otherwise agreed in writing between Motorola and Customer, the installation and implementation of accumulated backlog security patches and network updates is the responsibility of the Customer.
- If applicable, provide network connectivity at the zone core site(s) for Motorola to use to download and pre-position the software that is to be installed at the zone core site(s) and pushed to remote sites from there. Motorola will provide the network connection specifications, as listed in Section 1.4.1.2.4 Connectivity. Network connectivity must be provided at least 12 weeks prior to the scheduled System Upgrade. In the event access to a network connection is unavailable, the Customer may be billed additional costs to execute the System Upgrade.
- Assist in site walks of the system during the system audit when necessary.
- Provide a list of any FRUs and/or spare hardware to be included in the System Upgrade when applicable. Upon reasonable request by Motorola, Customer will provide a complete serial and model number list of the equipment. The inventory count of Customer FRUs and/or spare hardware to be included as of the start of the SUA is included in Section 1.6 Appendix B: System Pricing Configuration.
- Acknowledge that new and optional system release features or system expansions, and their required implementation labor, are not within the scope of the SUA. The Customer may purchase these under a separate agreement.
- Maintain an internet connection between the on premise radio solution and the cloud platform, unless provided by Motorola under separate Agreement.
- Identify any Customer specific standard or requirements that may be implicated by the planned upgrade(s), including heightened cloud, IT, or information security related standards or requirements, such as those that may apply to U.S. Federal Customer or other government Customer standards. Motorola makes no representations as to the compliance of ASTRO SUA with any Customer specific standards, requirements, specifications, or terms, except to the extent expressly specified.
- Participate in release impact training at least 12 weeks prior to the scheduled System Upgrade. This applies only to primary zone core owners. It is the zone core owner’s responsibility to contact and include any user agencies that need to be trained, or to act as a training agency for those users not included.

System Readiness Checkpoint

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

Motorola Responsibilities

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

Customer Responsibilities

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

System Upgrade

Motorola Responsibilities

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

Customer Responsibilities

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

Upgrade Completion

Motorola Responsibilities

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

Customer Responsibilities

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

1.4.1.10.5 Special Provisions

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

The SUA does not extend to customer-provided software and hardware. Motorola makes no warrants or commitments about adapting our standard system releases to accommodate customer implemented

equipment. If during the course of an upgrade, it is determined that customer provided software and/or hardware does not function properly, Motorola will notify the customer of the limitations. The customer owns any costs and liabilities associated with making the customer provided software and/or hardware work with the standard Motorola system release. This includes, but is not limited to, Motorola costs for the deployment of resources to implement the upgrade once the limitations have been resolved by the customer.

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

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

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

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

1.5 Appendix A: ASTRO 25 System Release Upgrade Paths

The upgrade paths for standard ASTRO system releases are listed in Table 1-21: Certified Standard ASTRO 25 System Release Upgrade Paths.

Table 1-21: Certified Standard ASTRO 25 System Release Upgrade Paths

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

The upgrade paths for high security ASTRO system releases for federal deployments are described in Table 1-22: Certified High Security ASTRO 25 System Release Upgrade Paths.

Table 1-22: Certified High Security ASTRO 25 System Release Upgrade Paths

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

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

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

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

1.6 Appendix B: System Pricing Configuration

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

Table 1-23: System Configuration

System Configuration	
Core Configurations	
Cloud based Core	0
On-premises Main Site	1
On-premises Backup Site	0
System Level Features	
Standalone servers (Critical Connect / Smart Connect)	1
NFM RTU (typically 1 per site location)	16
Network Management Clients	3
IMW Servers	0
Telephone Interconnect	0
Security Configurations	
AERSS Sensors	2
Firewalls	4

System Configuration	
KMF Servers	0
KMF Clients	0
RF Site Configurations	
Virtual Prime Sites (IP Simulcast Primes are separately proposed to be upgraded to Virtual Prime)	0
IP Simulcast Prime Sites (include co-located/redundant)	1
RF Sites (include Simulcast sub-sites, ASR sites, HPD sites)	15
GTR 8000 Base Stations	186
Dispatch Site Configurations	
Dispatch Site Locations	3
MCC 7500 Dispatch Consoles	29
AIS	2
CCGWs	5
MC EDGE Aux I/O	2
AXS Console Dispatch Site Locations (MCC 7500 are separately proposed upgrade AXS)	0
AXS Console PDH (Command Central Hub)	0
AXS Servers	0
Third Party Elements	
NICE Logging recorders (IP, Telephony, or Analog) Purchased through Motorola	0
MACH Alert FSA Purchased through Motorola	1
Genesis Applications Purchased through Motorola	1

1.7 Appendix C: SUA Coverage Table

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

Table 1-24: SUA Coverage Table

ASTRO Certified Solution	System Upgrade		
Equipment Provided by Motorola	**Software**	**Hardware Full Product**	**Hardware Board-Level**
Servers	✓	✓	
Workstations	✓	✓	
Firewalls	✓	✓	

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

1.8 Third Party Maintenance Services Detailed Description

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

1.8.1 Third Party Included Services

The following services are continued with the service renewal agreement.

Third Party Warranty Services	
Microwave Extended Aviat Care Support	✓
Microwave On-Site Support	✓
Fire Station Alerting Upgrade Agreement & Maintenance	✓
Genesis Support & Upgrade Agreement	✓
Vertiv UPS Service Agreement	✓
Tower RF Site Vegetation Control	✓
Generator & HVAC Service Support	✓

1.8.1.1 Microwave On-Site Support *

* NOTE: Microwave on-site support is included whether Fulton County chooses to or chooses not to refresh its microwave platform. If the microwave falls outside of Aviat support; Motorola on-site restoration and break-fix support and will revert to “best effort”. In this event; repairs will be billed on a time and material best effort basis. Motorola cannot guarantee restoration if platform is manufacturer end of support or end of life.

Bearcom, Motorola’s preferred authorized service partner, will support microwave on-site maintenance and restoration services.

Following proven response and restore processes, Motorola Solutions Dispatch contacts the local authorized service center in your area and dispatches a qualified technician to your site. An automated escalation and case management process ensures that technician site arrive and system restoration comply with contracted response times. The field technician restores the system by performing first level troubleshooting on site. If the technician is unable to resolve the issue, the case is escalated to the System Support Center or Aviat support product engineering teams, as needed.

1.8.1.2 Fire Station Alerting Upgrade Agreement & Maintenance

Fire Station Alerting (FSA) Support

Motorola Solutions proposed support extends Fulton County’s existing Mach Alert fire station alerting solution support for the next 10 years. During this period Motorola Solutions’ proposal includes the following services

Hardware Support, Board Repair, and Technical Support

- Remote terminal unit
- Alarm interface controller
- Servers
- Enhanced station controller
- Mushroom push button in NEMA 4 Box

Software and Technical Support

- Alarm interface controller
- Application software support for included software
- Software license

Fire Station Alerting (FSA) Mach Alert Upgrade Agreement

Mach Alert upgrades will coincide with ASTRO 25 proposed System Upgrade Agreement release deployments onto Fulton County's network. For Fulton County's FSA solution, Motorola Solutions will provide access to Mach Alert shipping software, required hardware upgrades, and implementation services. The software upgrades will be based on the Mach Alert server hardware utilized by Fulton County. If in the future, if Fulton County's version of the server is not supported by the Mach Alert software, newer supported equipment will be provided in order to accept the upgrade. Replacement or hardware refreshes of Fulton County's Fire Station located FSA equipment and platforms, including ASTRO 25 APX radios, are not included.

1.8.1.3 Genesis Support & Upgrade Agreement

Lifecycle Summary

This proposal is to renew the support and maintenance agreement covering Genesis software products and hardware for Fulton County. Support includes complete telephone and remote support or system analysis 8:00 am-5:00 pm Central Time, software updates & upgrades as well as after-hour emergency support for the specified term above. Hardware refresh(es) with a manufacturer warranty to cover the support term is included with on-site installation for ATIA systems or remote install for OTA systems. 3rd party software will be replaced if obsolescence occurs during term.

Software Products Covered

- GenWatch ATIA for single zone
- SAM
- GenWatch Data
- PMI

Hardware Provided Per Refresh

- Database/ DataProc Rackmount Server (1)
- Reader Rackmount Server (1)
- Desktop PC (1)

1.8.1.4 Vertiv UPS Service Agreement

Scope of Work:

- Uninterruptible Power Systems
- All Single Phase Models (Excluded NFinity)
- Essential Service – 1 Preventative Maintenance per contract year

Service Summary:

Feature	
On-Site Service	Includes 1 Preventive Maintenance Service, scheduled by the customer between 8am-5pm, Monday-Friday (excluding national holidays).
Response Time	Guaranteed 4-hour on-site emergency response, 7 days/week, 24 hours/day, within 150 miles of a Vertiv Services' Service City.
Customer Support	Includes access to the Customer Resolution Center (1-800-543-2378) and the Vertiv Customer Services Network Online Internet portal.
Parts	Includes parts coverage including internal batteries (limits may apply; see Assumptions and Clarifications, as applicable, for more details).
Labor & Travel	Includes 100% labor and travel coverage 7 days/week, 24 hours/day, within the 48 contiguous states and Hawaii.
Service Professional	Performed by Vertiv factory trained and authorized technician. Vertiv Services is the OEM service provider for Liebert products.

Services Performed:

UPS Full Preventive Maintenance Service

- Record the phase to phase and phase to neutral input voltages.
- Perform a temperature check on all breakers, connections, and associated controls. Repair and/or report all high temperature areas.
- Perform a complete visual inspection of the equipment, including sub-assemblies, wiring harnesses, contacts, cables and major components.
- Check all nuts, bolts, screws, and connectors for tightness and heat discoloration.
- Inspect for broken, brittle, damaged, or heat stressed components and cables.
- Clean any foreign material and dust from internal compartments.
- Perform a status check of alarm circuits.
- Perform an operational test of the system including unit transfer and battery discharge.
- Check or perform Engineering Field Change Notices (FCN) as necessary.
- Return the system to normal load and verify the output voltage. Calibrate as necessary.
- Review system performance with customer to address any system questions.

Battery Full Preventive Maintenance Service

- Check integrity of battery cabinet.

- Visually inspect battery system for: swelling, leaks, loose foreign objects, overheated or corroded cables and connectors, loose connections on batteries, and appropriate product labels related to safety and warning hazards.
- Clean and neutralize cell tops as required.
- Tighten all battery terminal connections to their proper specifications.
- Measure and record DC bus ripple voltage.
- Measure and record total battery float voltage.
- Record room ambient temperature.

Assumptions and Clarifications

- Parts coverage excludes air filters, proactive full bank capacitor replacement and fan replacement.

Fulton County Responsibilities

In order to provide timely, accurate and thorough execution of the services described herein, Vertiv requests the following:

- Point of Contact: Provide an authorized point of contact(s), specific for the scope of work, for scheduling and coordination purposes.
- Scheduling: Make dates available for scheduling service. All visits must be requested 10 business days in advance of need by contacting the Vertiv Services Customer Resolution Center at 1-800-543-2378.
- Site Access: Prior to time of scheduled work, provide site access including any customer required escort, security clearance, safety training and badging for Vertiv service personnel.
- Equipment Access: Convenient access to the equipment covered by the Scope of Work. Prior to scheduled time of work, notify Vertiv service personnel of any special requirements for equipment access including lifts, ladders, etc.
- Shutdown: Service may require shutdown of load to ensure electrical connection integrity.
- Notification: If for any reason the work cannot be performed during scheduled time, notify Vertiv service personnel 24-hours prior to scheduled event.

1.8.1.5 Tower RF Site Vegetation Control

Scope of Work:

Vegetation Management Services Overview

Motorola will provide vegetation management services for the below listed sites through an annual service program. The goal of this program is to control and prevent unwanted vegetation growth in non-turf areas. Services Provided Services include:

- Post-emergent weed treatments
- Pre-emergent weed prevention
- Bare ground vegetation control
- Fence lines and perimeter areas
- Application Methods Applications are performed by trained technicians using:
- Truck-mounted sprayers

- ATV-mounted sprayers
- Backpack sprayers Herbicide application.

Motorola Tower sites. Locations to be treated:

- FC Master Site New
  6000 Plummer Road, Atlanta, GA 30336
- FC Master Site Old
  6000 Plummer Road, Atlanta, GA 30336
- Freemanville Rd.
  16300 Freemanville Road, Alpharetta, GA 30004
- Roswell High School
  11595 King Road, Roswell, GA 30075
- Jones Bridge
  10735 Jones Bridge Road, Alpharetta, GA 30022
- Morgan Falls Park
  450 Morgan Falls Road, Atlanta, GA 30350
- Johns Creek
  6425 Old Atlanta Road, Suwanee, GA 30024
- Burdette Park
  5901 Deerfield Trail, College Park, GA 30349
- Fire Station
  178675 Ridge Road, Fairburn, GA 30213
- Palmetto
  505 Carlton Road, Palmetto, GA 30268
- JC Laramore
  5651 Stonewall Tell Road, Atlanta, GA 30349

1.8.1.6 Generator PM Service Support

Generator PMs include once yearly annual services consisting of a Comprehensive PM with exclusions as listed below.

Annual Comprehensive PM Services:

- **Lubrication**
  - Check engine crankcase oil level.
  - Visually check for coolant contamination.
  - Change engine oil and filters using multi-viscosity oil.
  - Clean crankcase breather.
  - Lubricate generator bearing.
- **Cooling System**
  - Check engine coolant level. Add coolant if level is low.
  - Inspect unit for a low coolant sensor. If unit is not equipped, note in recommendations.
  - Check Supplemental Coolant Additive (SCA).

- Inspect coolant line connections and hoses.
- Check fan/alternator belt tension and wear.
- Inspect the fan idler pivot and grease.
- Inspect the cooling fan and grease the drive bearing, and inspect the fan hub for proper clearance.
- Inspect the fan idler pulley assembly.
- Change coolant filter (if applicable).
- Inspect coolant block heaters' operation and record temperatures.
- Inspect coolant pump.

- **Fuel System**
  - Diesel Fuel Generators
    - Replace fuel filters.
    - Inspect main tank and day tank (if applicable).
    - Check piping and correct minor leaks.
    - Check motor and wiring for overheat.
    - Check pump and float switch for continuity.
    - Check level indicator (gauge) and indicate level in site glass.
  - Gaseous Generators
    - Inspect main tank and day tank (if applicable).
    - Check piping, valves, & fittings.
    - Correct minor leaks.
- **Air Induction and Exhaust**
  - Check air cleaner and service indicator.
  - Check/Clean dust collector cap.
  - Inspect manifold and air piping.
  - Inspect intake hoses and clamps.
  - Inspect intake and exhaust openings.
  - If equipped with automatic louver systems, verify automatic louver system operation. Ensure louvers are wired to generator.
- **Electrical System**
  - Check battery electrolyte.
  - Load test batteries and record findings.
  - Clean and inspect battery cables and electrical connections.
  - Inspect alternator drive belt(s).
  - Check shutoff controls.
  - Inspect starter.
  - Check cold weather starting aids.
  - Check battery charger operation. Make sure light indicator is correct and "green" is on.

- Record high and low rate in volts. Voltage tests are to be taken for battery charger (low) in OFF mode and for alternator charging (high) while the generator is running.
- Clean voltage regulator (if needed).
- Record battery date and date of battery replacement.

- **Engine and Alarm Verification and Testing**
  - Record engine crank time.
  - Record engine RPM voltage and adjust if necessary.
  - Record no load frequency and adjust if necessary.
  - Check and record engine oil pressure.
  - Check and record engine operating temperature.
  - Check and record engine charging system.
  - Check and record: Generator Instruments.
- **General Conditions**
  - Inspect all belts and ensure proper adjustment.
  - Inspect control panel for frayed or damaged wires.
  - Visually inspect the vibration damper for rips, tears, broken springs or leaks in liquid isolators.
  - Inspect the generator and engine hold down bolts.
  - Inspect the engine for oil and coolant leaks and note.
  - Record run hours.
  - Report condition of generator enclosure and exhaust system including leaks, holes, rust, etc.
  - Report overall condition of the area surrounding the generator.
  - Record whether ethylene or propylene glycol and the ratio.

Exclusions:

- Repair Call Outs including Mobilization, Parts and Labor are not included in this agreement.
- Replacement of non-repairable generator.
- Replacement or repair of fuel storage elements, transfer switches, or batteries.

Parts and labor for exclusions shall require separate quote and purchase.

1.8.1.7 HVAC PM Service Support

HVAC PMs include once yearly annual services consisting of services with exclusions as listed below.

Annual PM Services:

- Check Condenser/evap. Coils. (Both Sides)
- Replace compressor contactors.
- Check capacitor values.
- Change filter, date & initial. (CABINET/WAC&DAC sites, inspect/clean outside air intake panels and screens on heat exchangers & cabinet units.)

- Check the refrigerant charge.
- Check thermostats/ controller, electrical connections, drains, alarm connections, wiring, amp draw on motor's, set time/delay relays (2/5min.).
- Check to make sure the units are clear of debris, and ensure all panels are secure.
- Check the refrigerant charge

Exclusions:

- Repair Call Outs including Mobilization, Parts and Labor are not included in this agreement.
- Compressors and coils are not included in this agreement.
- Replacement of non-repairable HVAC.

Parts and labor for exclusions shall require separate quote and purchase.

1.9 Priority Level Definitions and Response Times

Table 1-25: Priority Level Definitions and Response Time describes the criteria Motorola uses to prioritize incidents and service requests, and lists the response times for those priority levels.

Table 1-25: Priority Level Definitions and Response Time

Incident Priority	Incident Definition	Initial Response Time	On-Site Response Time
Critical P1	▪ **Core:** Core server or core link failure. No redundant server or link available. ▪ **Sites/Subsites:** Primary site down. Two RF sites or more than 10% of RF sites down, whichever is greater. ▪ **Consoles:** More than 40% of a site's console positions down. ▪ **Conventional Channels:** Conventional Channel Gateways (CCGW) down without redundant gateways available. ▪ **Security Features:** Security is non-functional or degraded. ▪ **Alarm Events:** Door, motion, intrusion, power failure, or environmental alarms triggered.	Response provided 24/7 until service restoration. Technical resource will acknowledge incident and respond within 30 minutes of CMSO logging incident.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.
High P2	▪ **Core:** Core server or link failures. Redundant server or link available. ▪ **Consoles:** Between 20% and 40% of a site's console positions down. ▪ **Sites/Subsites:** One RF site or up to 10% of RF sites down, whichever is greater. ▪ **Conventional Channels:** Up to 50% of CCGWs down. Redundant gateways available.	Response provided 24/7 until service restoration. Technical resource will acknowledge incident and respond within 1 hour of CMSO logging incident.	Response provided 24/7 until service restoration. Field service technician arrival on-site within 4 hours of receiving dispatch notification.

Incident Priority	Incident Definition	Initial Response Time	On-Site Response Time
	▪ **Network Elements:** Site router, site switch, or GPS server down. No redundant networking element available.		
Medium P3	▪ **Consoles:** Up to 20% of a site's console positions down. ▪ **Conventional Channels:** Single channel down. Redundant gateway available. ▪ **Network Elements:** Site router/switch or GPS server down. Redundant networking element available.	Response provided during normal business hours until service restoration. Technical resource will acknowledge incident and respond within 4 hours of CMSO logging incident.	Response provided during normal business hours until service restoration. Field service technician arrival on-site within 8 hours of receiving dispatch notification.
Low P4	▪ **Service Requests:** Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).	Response provided during normal business hours. Motorola will acknowledge and respond within 1 Business Day.	Not applicable.

1.10 ASTRO 25 Remote Security Upgrade Service (RSUS) Coverage Appendix 1

1.10.1 RSUS Coverage

The following table defines which components are covered by the Remote SUS service.

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

Table 1-26: RSUS Covered Components

SOFTWARE	UPDATE RELEASE CADENCE	PRODUCTS * DEPENDS ON DEVICE NETWORK LOCATION IN RNI OR CONNECTIVITY SETTINGS *
Antivirus Definition Files	Weekly	▪ Based on automated (CSMS) Core Security Management Server configurations
Microsoft Windows	Monthly	▪ (AMS) Advanced Messaging Server ▪ (AuC) Authentication Center Client ▪ (AuC) Authentication Center Server ▪ (CSMS) Core Security Management Server ▪ (DC) Domain Controller ▪ (IPPBX) (ETI) Enhanced Telephone Interconnect ▪ (KMF) Key Management Framework Client ▪ (KMF) Key Management Framework Server ▪ (MCC) Master Control Console 5500 ▪ (MCC) Master Control Console 7100 ▪ (MCC) Master Control Console 7500 / (AIS) Archiving Interface Server ▪ (MCC) Master Control Console 7500 E ▪ (MCC) Master Control Consoles 7500 E ▪ (NM) Network Management Client ▪ (OPSOC) On-Prem Security Operations Center ▪ (RM) Radio Management Client ▪ (RM) Radio Management Server ▪ MACH Alert (FSA) Fire Station Alerting ▪ Marvlis AVL Desktop Monitor ▪ Marvlis Server ▪ NICE (AIS) Archiving Interface Server ▪ NICE Backup Server ▪ NICE IP Radio Logger ▪ NICE Replay Workstation ▪ Proxy 7000 ▪ Transcoder

SOFTWARE	UPDATE RELEASE CADENCE	PRODUCTS * DEPENDS ON DEVICE NETWORK LOCATION IN RNI OR CONNECTIVITY SETTINGS *
		▪ Verint Logging Recorder Server ▪ Verint Workstation
Microsoft Windows SQL Server	Quarterly	▪ (CSMS) Core Security Management Server
Red Hat Linux (RHEL)	Quarterly	▪ (ATR) Air Traffic Router ▪ (BAR) Backup and Restore Server ▪ (IPCAP) IP Packet Capture ▪ (ISGW) Intersystem Gateway ▪ (LM) License Manager ▪ (LMP) LMP Multicast Proxy ▪ (NTP) Network Time Protocol ▪ (PDG) Packet Data Gateway ▪ (SSS) System Statistical Service ▪ (Syslog) Syslog Service ▪ (UCS) User Configuration Server ▪ (UEM) Unified Event Manager ▪ (UNC) Unified Network Configurator ▪ (ZC) Zone Controller ▪ (ZDS) Zone Database Service ▪ (ZSS) Zone Statistical Server
VMWare ESXi Hypervisor	Quarterly	▪ (VMS) Virtual Management Server
VMWare vCenter	Quarterly	▪ (VCLS) vSphere Cluster Services
McAfee/Trellix Patch(es)	Quarterly	▪ (CSMS) Core Security Management Server
Dot Hill DAS Firmware	Quarterly	▪ 4524 ▪ 4525
HP SPP Firmware	Quarterly	▪ HP Generation 9 ▪ HP Generation 10

1.10.2 Exclusions

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

Table 1-27: Excluded Components

Software	Products
Product Lines	▪ (IMW) Intelligent Middleware Server ▪ WAVE Radio Gateway ▪ WAVE Tactical ▪ (PA) Personnel Accountability

Software	Products
	▪ (CEN) Customer Enterprise Network Located Loggers (including Telephony)
Antivirus Definition Files	▪ Stand Alone Deployed Products
Microsoft Windows	▪ (CAM) Console Alias Manager Server ▪ Genesis Genwatch3 ▪ GenesisWorld Performance Management Solutions Client
Microsoft Windows SQL Server	▪ NICE IP Logging Recorder
QNAP	▪ TS453A ▪ TS453Be ▪ TS453D ▪ TS-464
PostgreSQL	▪ (KMF) Key Management Framework Server
McAfee/Trellix Patch(es)	▪ Stand Alone Deployed Products

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

1.11 Fulton County Maintenance and SUA Renewal

1.11.1 Overview

The Motorola Solutions, Inc. (“Motorola Solutions”) System Manager (“SM”) service provides a dedicated resource that is responsible for delivering Technical Services as herein defined. The resource will be available to the Customer based on predefined schedules as set forth in this Statement of Work (“SOW”).

Pursuant to the terms and conditions of the applicable agreement, together with all applicable addenda (“Agreement”) between Motorola Solutions and the customer (“Customer”), this SOW defines the principal activities and responsibilities of all parties in the delivery of System Manager services.

In the event of a conflict between the terms and conditions of an Agreement and the terms and conditions of this SOW, this SOW will control as to the inconsistency only.

1.11.2 Description of Services

Motorola Solutions’ dedicated SM assists in the management of the Customer’s communications network. The SM acts as communications liaison and coordinator of the services listed on the Agreement. The SM serves as the primary Motorola contact who will work closely with the Customer, and any additional required parties. The SM may reside on-site at the Customer’s location, or work from a Motorola facility or remote location, and visit the Customer’s location on a schedule determined between the Customer and the SM.

The SM will be provided a mix of on-the-job and formal training to accomplish the tasks outlined in this document. With Customer’s guidance, the SM will develop an understanding of the assigned agency’s specific environment, Customer-specific requirements, and customizations. The SM will act as the interface between Motorola software and hardware technical support teams to achieve the goals outlined by their respectively assigned Customer.

Below are some responsibilities that Customers may typically want performed by their SM. This list is not exhaustive and any final responsibilities should be agreed upon between the Customer and the SM and captured in the applicable Agreement.

1.11.2.1 Motorola Solutions Responsibilities

1.11.2.1.1 Administrative Support

- Serve as the main point-of-contact for support related to Customer’s Motorola Solutions Radio System.
- Coordinate with Motorola Solutions and/or Customer Project Management (“PM”) as applicable.
- Assist in the development of internal documentation pertaining to system configuration, administration, and troubleshooting.
- Help develop local agency/user surveys.
- Helps ensure that Motorola Solutions installed equipment is maintained with FCC and Customer stipulated requirements.

- Provide dedicated support full-time, minus Motorola Solutions and Customer holidays, paid time off (“PTO”) benefits, sick leave, and training events, outlined in the Resource Training section below, throughout the term of this agreement.

1.11.2.1.2 Radio System Configuration Management

- Advise and assist in development of document configuration requirements:
  - Technology requirements and capability.
  - Interoperability requirements.
  - Programming requirements.
  - Operational requirements.
  - Special situation reconfiguration requirements.
- Maintain Motorola Solutions system configuration records.
- Site documentation/ PM records.

1.11.2.1.3 Motorola Radio System Database Management and Oversight

- Advise and assist in managing SmartZone Database.
- Manage Data System Database.
- Manage MOSCAD Database.

1.11.2.1.4 Dispatch Services

- Assist with procedures for Dispatch Services.
- Dispatch local support and repair personnel as required based on the severity.
- Ensure that reported incidents or problems are documented, analyzed, validated, and escalated through full resolution when necessary.
- Update records, severity, and escalation information.
- Advise Motorola of changes to escalation information.
- In cases where the SM has responded to system failure or critical issues, verify with Customer that restoration is complete and/or system is functional.

1.11.2.1.5 On-Site Technical Support

- Run diagnostics using approved Motorola Solutions tools.
- Work with Customer staff to identify and resolve reported system incidents/problems.

1.11.2.1.6 Advise and Assist with Radio and Infrastructure Repair

- Establish depot repair procedures.
- Implement a process for repairs.
- Maintain spare device swap procedure.
- Establish/review procedure to notify users of repair status.
- Manage emergency repair efforts and escalation procedures.

- Repair bank management.

1.11.2.1.7 Radio Network Remote Diagnostics

- Review system dial-in capability.
- Review depth of diagnostic capability.
- Review system network connection and capability.

1.11.2.1.8 Service Agreement Management

- Maintain annual service agreement:
  - Additions/deletions.
  - Price changes.
- Review pricing with the Customer during renewal period.

1.11.2.1.9 Site Maintenance

- Oversee Motorola Solutions provided and installed infrastructure preventive maintenance activities.
- Recommend maintenance procedures and requirements.
- Monitor scheduled downtime.
- Coordinate with outside services/supplier to site for:
  - Telephone circuits.
  - AC power.
  - Tower structure.
  - Power generator.
  - Property maintenance.

1.11.2.1.10 System Documentation

- Maintain radio system documentation.
- Maintain operational and technical manuals.

1.11.2.1.11 System Infrastructure Performance Reporting

- Maintain records from service providers.
- Provide device performance report:
  - Planned and unplanned downtime.
  - Root cause analyses.
  - Fault Management integration with other alarm systems.
- Provide system airtime usage report.
- Provide system performance reports and analysis.

- Gather data from reporting resources and prepare Performance Reports as required and/or requested.
- Track system alarms and response.

1.11.2.1.12 System Planning

- Review new and replacement equipment purchases.
- Review organizational goals and objectives.
- Identify wireless role in achieving the goals and objectives.
- Oversee the implementation of all system upgrades performed by Motorola Solutions to ensure total continuity and minimal system impact.
- Maintain awareness of Software Maintenance Agreement ("SMA") bulletins and engage the appropriate Motorola Solutions resources for System Release upgrades.
- Assist with upgrade planning and installations.
- Understand system dependencies and related connections.
- Identify opportunities for long-term growth and strategic planning of the Customer's system.

1.11.2.1.13 Event Planning

- Preparation Disaster/Crisis recovery plan:
  - "What-If" Scenarios.
  - Backup Communications.
  - Equipment Rental Plans.
  - System Service Response Plan.
- Communicate plans to users and management.
- Assist in system studies.
- Assist with contractually covered database system backups.

1.11.2.1.14 Technical Support

- Provide technical and managerial assistance during critical response situations.
- Contact Call Center when a problem occurs and provide System ID, a description of the problem, and contact information.
- Diagnose, triage, gather logs, and coordinate with Motorola Solutions Technical Support, Motorola Solutions Engineering teams, and contractually agreed upon third-party vendors to resolve reported system incidents/problems.

1.11.2.1.15 Training

- Advise the Customer with training plan development for users and system functionalities. Engage appropriate Motorola Solutions subject matter experts ("SMEs") when necessary.
- Coordinate on-site training if applicable.
- Coordinate classroom technology training if applicable.

- Coordinate train-the-trainer training if applicable.

1.11.2.1.16 User Support and Interaction

- Establish procedures to review user needs.
- Establish procedures to respond to end user system questions and concerns.
- Assist and advise the customer in preparing an end-user survey and feedback.
- Advise the customer to develop a user group committee to review needs, survey results and improvements.
- Assist the customer in setting up regular meetings with user groups regarding system performance and capabilities.

1.11.2.1.17 Vendor Management

- Review current service agreements scope and suppliers:
  - Implement quality standards and procedures.
- Contract administration.
- Coordinate provision of third party/vendor services.
- Engage third-party vendors to provide contracted services in connection with issues causing a system failure, when applicable. This may include some instances involving third-party vendor on-site support as well as coordination of third-party upgrade services, when applicable.
- Coordinate with outside services/supplier to site for:
  - Telephone circuits.
  - AC power.
  - Tower structure.
  - Power generator.
  - Property maintenance.
- Qualified vendor monitoring:
  - Qualified vendor service quality data collection.
  - Compliance/Adherence monitoring.
  - Vendor’s quality programs.
- Warranty processing.

1.11.2.1.18 Field Service Bulletin Responsibilities / Patching Services

- Complete all patching including Security Technical Implementation Guide (“STIGs”) and anti-virus.
- Perform periodic system maintenance and software patching, in accordance with Motorola Solutions supplied guidelines, on physical and virtual servers covered within the scope of the Maintenance and Service Agreement.
- Review and execute Motorola Technical Notifications (“MTNs”) as necessary.

1.11.2.1.19 Other Responsibilities

- Manage meetings between Customer and Motorola Solutions.
- Provide site access to third-party vendors, as approved by Customer.
- Manage Customer's dedicated team.
- Acquire quotes from vendors.
- Present quotes to Customer.
- Process Motorola Solutions work tickets for billing.
- Address Motorola Solutions billing issues.
- Work with pre-sale/post-sale engineering.
- Work with the Project or Program Manager on project execution.
- Create Methods of Procedures ("MOPs") with Customer.
- Create Purchase Orders ("Pos") for vendors, as approved by Customer.
- System downtime scheduled/un-scheduled email notifications.
- Provide recommendations for systems improvement.

1.11.2.2 Customer Responsibilities

- Upon report of any incident/problem, provide pertinent and specific details of the issue, as well as information regarding actions already taken.
- Allow the SM full and free access to equipment, including any connectivity/monitoring equipment, necessary to deliver the services outlined in this SOW.
- Provide all information pertaining to external hardware and software that covered products interface with to enable the resource to perform their obligations under this Agreement.
- Initially report all active incidents or technical requests of any Severity to the Technical Support Organization at 800-MSI-HELP to obtain a case number. Provide the case number to SM.
- Allow Motorola Solutions continuous remote access to the system, and to obtain system availability and performance data.
- Notify SM and Motorola Solutions Technical Support when performing any activity that impacts the system. (This may include but is not limited to, installing software or hardware upgrades, performing network maintenance or upgrades, disabling system peripherals to perform maintenance, etc.). Note: Motorola Solutions is not responsible for loss of functionality or other technical disruptions stemming from system impacting activity not performed by Motorola Solutions personnel.
- Maintain and store all relevant software and system backups in an easily accessible location. Motorola Solutions recommends that at least one backup file is stored in an off-site location.
- Coordinate and assist with troubleshooting efforts and restoration attempts during cases in which the SM is responding to a system failure.
- Provide the SM, at no charge, a non-hazardous environment including shelter, heat, light, power, and all other reasonable accommodations.
- Validate issue resolution in a timely manner, prior to closure of the incident/problem.

- Adhere to all other applicable guidelines referenced in the separate Motorola Solutions Customer Support Plan (“CSP”).
- Assist in agency-specific knowledge development for the SM.
- Provide SM a central point-of-contact that is available and accessible to Motorola Solutions twenty-four (24) hours a day. This contact shall be authorized to act and make decisions on behalf of Customer, with regard to a Motorola Solutions response and for coordinating the system calls.

1.11.3 Resource Training

In order to maintain and expand product and technical knowledge as our technologies and Customer environments evolve, the SM will be required to attend up to 80 hours of annual training. Some training may be available on a remote basis, but other training will require the SM to travel to a remote site to complete training. On-going training is designed to enhance and expand the SM’s knowledge and capabilities in an effort to continuously improve the services provided. Motorola Solutions will provide adequate advanced notice, generally 30 days, of any training requirements for the SM.

1.11.4 Dedicated System Manager Placement

Motorola Solutions will make a good faith effort to secure a local resource with suitable abilities and qualifications for the duration of the Agreement. If Customer objects in good faith to a proposed System Manager assignment, the Parties shall attempt to resolve Customer’s concerns on a mutually agreeable basis.

In the event Motorola Solutions is unable to propose a Dedicated System Manager that Customer in good faith finds qualified, Customer can terminate this Agreement. Motorola Solutions will provide a prorated credit based upon the remaining term of the Agreement.

Customer may request Motorola Solutions remove and replace a System Manager for any valid performance or business reason, provided that the Customer does not request the removal of any such person for reasons prohibited by law, and further provided that reasonable notice (which may be immediate, depending on the circumstances surrounding the removal) is given.

In the event Customer refuses the placement or requests removal of a qualified System Manager, Motorola Solutions shall have the right to terminate the Agreement in whole or in part and immediately escalate any remaining amounts due under the Agreement, if any.

Section 2

Pricing

2.1 Pricing Summary

Payment Summary for SUA and Maintenance Contract	
Proposed Renewal Contract	
Initial 3 Month Term (October 2026-December 2026)	$387,0000
Year One: 2027	$1,901,181
Year Two: 2028	$1,901,181
Year Three: 2029	$1,901,181
Year Four: 2030	$1,901,181
Year Five: 2031	$1,901,181
Year Six: 2032	$1,901,181
Year Seven: 2033	$1,901,181
Year Eight: 2034	$1,901,181
Total SUA and Maintenance Contract:	**$15,596,448**

2.2 Payment Schedule

Except for a payment that is due on the Effective Date, Customer will make payments to Motorola within thirty (30) days after the date of each invoice. Customer will make payments when due in the form of a check, cashier's check, or wire transfer drawn on a U.S. financial institution. If Customer has purchased additional Professional or Subscription services, payment will be in accordance with the applicable addenda.

Motorola will invoice Customer annually in advance of each year of the plan in accordance with the pricing summary.

INFLATION REVIEW. For multi-year agreements, at the end of the first year of the Agreement and each year thereafter, a CPI percentage change calculation shall be performed using the U.S. Department of Labor, Consumer Price Index, "All Items," Unadjusted Urban Areas (CPI-U). Should the annual inflation rate increase greater than 3% during the previous year, Motorola shall have the right to increase all future maintenance prices by the CPI increase amount exceeding 3%. "All Items," not seasonally adjusted shall be used as the measure of CPI for this price adjustment. The adjustment calculation will be based upon the CPI for the most recent twelve (12) month increment beginning from the most current month available as posted by the U.S. Department of Labor (http://www.bls.gov) immediately preceding the new maintenance year. For purposes of illustration, if in Year 5 the CPI reported an increase of 8%, Motorola may increase the Year 6 price by 5% (8%-3% base). Any pricing change would be documented in a change order executed with the Customer.