



East Bay Regional Communications System Authority



Participating agencies include Alameda and Contra Costa Counties and the following cities and special districts: Alameda, Albany, Antioch, Berkeley, Brentwood, Clayton, Concord, Danville, Dublin, El Cerrito, Emeryville, Fremont, Hayward, Hercules, Lafayette, Livermore, Martinez, Moraga, Newark, Oakley, Pinole, Pittsburg, Pleasant Hill, Pleasanton, Richmond, San Leandro, San Pablo, San Ramon, Union City, Walnut Creek, East Bay Regional Park District, Kensington Police Community Services District, Livermore Amador Valley Transit Authority, Moraga-Orinda Fire District, Rodeo-Hercules Fire District, San Ramon Valley Fire District, California Department of Transportation, Ohlone Community College District, Contra Costa Community College District, Dublin-San Ramon Services District and University of California, Berkeley

OPERATIONS COMMITTEE MEETING

NOTICE OF SPECIAL MEETING

DATE: September 15, 2023

TIME: 10:00 a.m.

PLACE: Alameda County Office of Homeland Security and Emergency Services,
Room 1013
4985 Broder Blvd., Dublin, CA 94568

AGENDA

1. Call to Order/Roll Call
2. Public Comments (Meeting Open to the Public):
At this time, the public is permitted to address the Committee on items within the Committee's subject matter jurisdiction that do appear on the agenda. Please limit comments to a maximum of three (3) minutes.
3. Approval of Minutes of June 2, 2023, Operations Committee Meeting
4. Motorola SUA and Maintenance Agreement
5. Contra Costa County ITD Service Agreement
6. Request Direction regarding Recruitment of Executive Director
7. Updates on East Bay Regional Communications System Projects
 - Time Division Multiple Access (TDMA)
 - Encryption
 - Microwave/MPLS
 - The City of Antioch Site on Walton Lane
 - Carquinez Site Completion
 - Wiedemann Project San Ramon
 - Alameda County Parking Lot next to East Dublin BART
8. Agenda Items for Next Meeting

**Alameda County Office of Homeland Security and Emergency Services
4985 Broder Blvd, Dublin CA 94568 • (925) 803-7802 • www.ebrcsa.org**

- Aviat Repair and Maintenance Agreement

9. Adjournment

This AGENDA is posted in accordance with Government Code Section 54954.2(a)

If requested, pursuant to Government Code Section 54953.2, this agenda shall be made available in appropriate alternative formats to persons with a disability, as required by Section 202 of the Americans with Disabilities Act of 1990 (42 U.S.C. Section 12132), and the federal rules and regulations adopted in implementation thereof. To make a request for disability-related modification or accommodation, please contact the EBRCSA at (925) 803-7802 at least 72 hours in advance of the meeting.

I hereby certify that the attached agenda was posted 24 hours before the noted meeting.

A handwritten signature in black ink that reads "Tom McCarthy". The signature is written in a cursive, slightly slanted style.

Tom McCarthy, Executive Director
September 11, 2023



**East Bay Regional
Communications
System Authority**



Participating agencies include Alameda and Contra Costa Counties and the following cities and special districts: Alameda, Albany, Antioch, Berkeley, Brentwood, Clayton, Concord, Danville, Dublin, El Cerrito, Emeryville, Fremont, Hayward, Hercules, Lafayette, Livermore, Martinez, Moraga, Newark, Oakley, Pinole, Pittsburg, Pleasant Hill, Pleasanton, Richmond, San Leandro, San Pablo, San Ramon, Union City, Walnut Creek, East Bay Regional Park District, Kensington Police Community Services District, Livermore Amador Valley Transit Authority, Moraga-Orinda Fire District, Rodeo-Hercules Fire District, San Ramon Valley Fire District, California Department of Transportation, Ohlone Community College District, Contra Costa Community College District, Dublin-San Ramon Services District and University of California, Berkeley

AGENDA ITEM NO. 3.

**AGENDA STATEMENT
OPERATIONS COMMITTEE SPECIAL MEETING
MEETING DATE: September 15, 2023**

TO: Operations Committee
East Bay Regional Communications System Authority (EBRCSA)

FROM: Tom McCarthy, Executive Director
East Bay Regional Communications System Authority

SUBJECT: Approval of Minutes of the June 2, 2023, Regular Operations Committee Meeting

RECOMMENDATIONS:

Approve the minutes of the June 2, 2023, Regular Operations Committee meeting.

SUMMARY/DISCUSSION:

The Operations Committee will consider approval of the minutes of the June 2, 2023, Regular Operations Committee meeting.

RECOMMENDED ACTION:

It is recommended that the Committee approve the minutes of the June 2, 2023, Operations Committee meeting.

Attachment:

Attachment "A"- Draft Minutes June 2, 2023, Operations Committee Meeting



East Bay Regional Communications System Authority



Participating agencies include Alameda and Contra Costa Counties and the following cities and special districts: Alameda, Albany, Antioch, Berkeley, Brentwood, Clayton, Concord, Danville, Dublin, El Cerrito, Emeryville, Fremont, Hayward, Hercules, Lafayette, Livermore, Martinez, Moraga, Newark, Oakley, Pinole, Pittsburg, Pleasant Hill, Pleasanton, Richmond, San Leandro, San Pablo, San Ramon, Union City, Walnut Creek, East Bay Regional Park District, Kensington Police Community Services District, Livermore Amador Valley Transit Authority, Moraga-Orinda Fire District, Rodeo-Hercules Fire District, San Ramon Valley Fire District, California Department of Transportation, Ohlone Community College District, Contra Costa Community College District, Dublin-San Ramon Services District and University of California, Berkeley

OPERATIONS COMMITTEE MEETING

SPECIAL MEETING

DATE: June 2, 2023

TIME: 10:00 a.m.

PLACE: Alameda County Office of Homeland Security and Emergency Services,
Room 1013
4985 Broder Blvd., Dublin, CA 94568

DRAFT MINUTES

-
- 1. Call to Order/Roll Call: 10:00 a.m.**
 - 2. Public Comments (Meeting Open to the Public):**
 - 3. Approval of Minutes of October 14, 2022 Operations Committee Meeting**

On motion of Bm. King, seconded by Bm. Christy and by unanimous vote, the Operations Committee approved the minutes of the October 14, 2022 Operation Committee meeting.

- 4. Budget Review FY 2023/2024**

Craig Boyer, Auditor, stated the first page of the budget document shows summary of the revenues and expenses for the upcoming fiscal year; revenues are derived based on the rate structure that is in effect times the number of radios. Historically, the Authority has seen an increase as they brought more members onto the JPA, but recently membership has plateaued and so any increases would primarily be driven by the rate structure, so, given that the rated structure has not changed since the prior year, the revenue estimate for this coming fiscal year is pretty consistent with the current fiscal year. On the expense side, a lot of the expenses are driven by contract costs. Where they have contracts in place, they use the actual contract numbers, otherwise they use an inflation factor - this year 4% for their assumption for those costs where they do not have contract rates in effect. If you compare costs with current year, a lot of operating costs have been impacted by the recent inflation so there are increases there. Capital varies from year-to-year. On page 2, there is a more detailed breakdown of all the expenses by different categories so you can see where the changes are happening. In the capital section, they list out all the different projects that are being budgeted for prior year, current and upcoming fiscal year. The first column shows last year's budget, the second column

**Alameda County Office of Homeland Security and Emergency Services
4985 Broder Blvd, Dublin CA 94568 • (925) 803-7802 • www.ebrcsa.org**

shows projected budget and there are still a couple months of activity. Third column is budgeted numbers, and the fourth column shows where they expect to land this year as to where they are budgeting for next year. There are increases in operating costs. On the capital side there is a bump up but they did reclassify one of the line items that used to be shown as an operating cost, so if you back that out, capital is flat. The third page shows the reserve balances for the Authority. The Authority has certain amount of monies that are not obligated to any specific purpose, but the Authority has policies in place that say they have to fund certain reserves. There are three reserve categories, the first being an operating reserve, which is required to be funded at 50% of what is budgeted. Then there is the debt service reserve, as long as the debt is outstanding, it is required to be budgeted at \$1 million. Anything that is left over goes into the capital reserve with the expectation that it will be used for capital. The final page is the 10-Year cash flow projection. They are fairly conservative on how this is done. It is to see whether or not the current rate structure meets the Authority's needs. On the revenue side, they do not assume any increases in member dues. You can see on a year-by-year basis, how the reserved balances are changing with the assumption of no changes in the rate structure. Currently, based on the current rate structure, the reserves should stay fairly stable. They have only put in capital costs that they know about. If there are other items coming down the pipeline, then these amounts change. But with what they currently know, it shows the Authority has stable reserve balances.

On motion of Bm. King, seconded by Bm. Vorhauer and by unanimous vote, the Operations Committee agreed to recommend to the Board the approval of the proposed FY 23/24 annual EBRCSA budget.

5. Hayward Annex Replacement Antenna

Executive Director McCarthy stated they surveyed all the sites for the microwave upgrade and discovered that the mount that holds the dish on the tower needs to be taken down. Motorola stated they came up with a price of \$45,000 to change out the dish, mount, and get it realigned.

On motion of Bm. Love, seconded by Bm. King and by unanimous vote, the Operations Committee agreed to recommend to the full Board the replacement of the Hayward Annex Microwave Dish and mounting hardware.

6. Aviat Purchase Order to Support Purchase and Repair of Existing Equipment, as Needed

This \$45,000 PO is for advance part replacement. If a router or server goes out, and the System needs a replacement, then Aviat will send a replacement. This is a bridge until the Executive Director redoes the agreement. It is a not-to-exceed amount of \$45,000.

On motion of Bm. King, seconded by Bm. Vorhauer and by unanimous vote, the Operations Committee agreed to recommend to the full Board the creation of a Purchase Order with Aviat to support purchase and repair of existing microwave equipment, as needed.

7. Request Direction regarding CHP Request for Access to EBRCSA

Executive Director McCarthy stated CHP requested access to EBRCSA because they back up law enforcement in the area. CHP wants to put 700 radios on the System at no cost to them. CHP is not encrypting their channels so they would not have communication with agencies that are encrypted. They said they will have mutual aid channel. They are trying to work out 10 radios for sideshow.

By consensus, the Operations Committee agreed that if CHP would like to bring forward a plan that includes payment for use of the System and it is acceptable, then they would consider it for recommendation to the Board.

8. Updates on East Bay Regional Commination System Projects

- Time Division Multiple Access (TDMA)

The Authority has done all the System work; there are some agencies that have not done their part in regard to purchasing radios or equipment.

- Encryption

The Authority has encrypted every console, and is finishing up the fleet maps. It will then be up to agencies to get radios programmed.

- Microwave/MPLS

Alameda County Microwave upgrade has been completed and will be starting the MPLS in two weeks.

- The City of Antioch Site on Walton Lane

There is a dead spot in Antioch at Walton Lane and the City and the Authority are trying to establish a new site there. Now there is a need for a seismic geo analysis and a tower survey. The Executive Director and the Authority's attorney are working on an agreement with the City of Antioch.

- Contra Costa County Site in Martinez Replacing 651 Pine Street

Equipment from the old site at 651 Pine Street will go to the Walton Lane site in Antioch site once the new Contra Costa County site is on.

- Wiedemann Project San Ramon

They hope to be ready to go in 30-45 days. It will clean up a lot of dead spots.

- Alameda County Parking Lot next to East Dublin BART

Alameda County is building a five-story parking lot at the East Dublin BART station. It will block the current tower. He will work with BART and will need to move them higher.

9. Agenda Items for Next Meeting

- Service Upgrade Agreement and Maintenance Agreement with Motorola

This 10-year agreement will end at the end of June.

- Aviat Repair and Maintenance Agreement

10. Adjournment: With no further business coming before the Operations Committee, the meeting was adjourned at 10:56 a.m.



**East Bay Regional
Communications
System Authority**



Participating agencies include Alameda and Contra Costa Counties and the following cities and special districts: Alameda, Albany, Antioch, Berkeley, Brentwood, Clayton, Concord, Danville, Dublin, El Cerrito, Emeryville, Fremont, Hayward, Hercules, Lafayette, Livermore, Martinez, Moraga, Newark, Oakley, Pinole, Pittsburg, Pleasant Hill, Pleasanton, Richmond, San Leandro, San Pablo, San Ramon, Union City, Walnut Creek, East Bay Regional Park District, Kensington Police Community Services District, Livermore Amador Valley Transit Authority, Moraga-Orinda Fire District, Rodeo-Hercules Fire District, San Ramon Valley Fire District, California Department of Transportation, Ohlone Community College District, Contra Costa Community College District, Dublin-San Ramon Services District and University of California, Berkeley

AGENDA ITEM 4.

**AGENDA STATEMENT
OPERATIONS COMMITTEE SPECIAL MEETING
MEETING DATE: September 15, 2023**

TO: Operations Committee
East Bay Regional Communications System Authority (EBRCSA)

FROM: Tom McCarthy, Executive Director
East Bay Regional Communications System Authority

SUBJECT: Consider Approval of a System Upgrade Agreement (SUA II), Maintenance Agreement, Multi Packet Label System (MPLS), Managed Detection and Response (MDR), and NICE (SUA II) with Motorola Solutions, Inc. to Provide System Technology Refresh including Hardware and Software for the EBRCSA System, and Authorization of its Execution and Implementation

RECOMMENDATIONS:

Request Committee discuss and make a recommendation to the Board of Directors regarding System Upgrade Agreement (SUA II) for the Master Site, Prime Sites, and NICE Logging System. The agreement includes combining the Maintenance agreement and SUA II as one agreement. The agreement also adds Multi Packet Label System (MPLS), Managed Detection and Response (MDR) with Motorola Solutions, Inc. The agreement will have Motorola Solutions, Inc. perform necessary upgrades and maintenance for the Master Site and Prime Sites. The SUA II has been used to maintain the East Bay Regional Communications System Authority (EBRCSA) system for the past 10 years.

SUMMARY/DISCUSSION:

The East Bay Regional Communications System Authority (EBRCSA) had two contracts with Motorola Solutions, Inc. which expired on June 30, 2023. The first was the SUA II which

provided upgrades in technology, software, and hardware extending the operational life of the System. The second was maintenance/repair for the Master Site and Prime Sites.

The SUA II system software releases cover base stations, site controllers, comparators, routers, LAN switches, servers, dispatch consoles, NICE logging equipment, network management terminals, Network Fault Management (“NFM”) products, network security devices such as firewalls, and intrusion detection sensors, and associated peripheral infrastructure software. The SUA II also provides hardware replacement for system components that must be replaced because of software upgrade, this includes servers, PC workstations, routers, and LAN switches. The SUA II does not include the replacement of dispatch consoles.

EBRCSA is adding Managed Detection and Response (MDR) with Motorola Systems, Inc. as a precaution due to recent events involving EBRCSA member agencies which were hacked. Due to the physical connection with agencies, we utilize various firewalls to protect EBRCSA. We want to include MDR to have monitoring which will allow EBRCSA to see attempts to access the System. Motorola Systems, Inc. is prepared to perform this monitoring and is prepared to monitor the system. In addition, as SUA II performs updates and changes to the System. They will ensure that the MDR works with the changes. Motorola Solutions, Inc. updates its system and security patches utilizing its connection to EBRCSA. Third party vendors are not allowed to connect to EBRCSA’s closed system. MDR will provide 24/7 monitoring and the ability to connect with the designated EBRCSA 24/7.

Motorola Solutions, Inc., in the original SUA II, had included NICE Logging as part of the agreement. In this agreement, NICE Logging is a separate part of the proposal. The NICE Logging is a third-party vendor authorized by Motorola Solutions, Inc.

FISCAL IMPACT:

If the Committees recommends this Agreement to the Board of Directors, this will require EBRCSA to increase the cost per radio. EBRCSA and the Auditors’ Office will prepare a recommendation concerning the increase in the subscriber fees. EBRCSA will include other contracts such as Aviat, East Bay Municipal Utility District, and other costs so that we maintain the recommended reserves.

The cost of the now expired SUA II was \$978,249 per year and Maintenance was \$1,437,000. The SUA II originally was set for 10 years at that cost and did not include increases each year. The Maintenance agreement was reviewed every three years and increased.

	2023/24	2024/25	2025/26	2026/27	2027/28	2028/29	TOTAL
ASTRO Maintenance	\$1,478,718	\$1,537,867	\$1,599,381	\$1,663,410	\$1,729,952	\$1,799,156	\$9,808,484
ASTRO SUA	\$1,368,746	\$1,401,210	\$1,434,973	\$1,470,086	\$1,506,604	\$1,544,583	\$8,726,201
MPLS	\$96,455	\$100,313	\$104,325	\$108,498	\$112,838	\$129,416	\$651,846
MDR	\$290,154	\$301,760	\$313,830	\$326,384	\$339,439	\$353,016	\$1,924,583
NICE SUA and Maintenance	\$322,951	\$286,144	\$306,213	\$327,802	\$351,032	\$376,039	\$1,970,180
TOTAL	\$3,557,023	\$3,627,293	\$3,758,723	\$3,896,180	\$4,039,866	\$4,202,211	\$23,081,295

See attached Agenda Item 4B, the budget amendment to the FY23-24 budget. Each of the five line items has been added as a separate line item on the second page schedule. Please review the cash flow projection on page 4. EBRCSA takes a conservative approach where it assumes no increase in dues from the current dues structure but applies a 4% increase to expenses annually unless EBRCSA has a contract amount that EBRCSA can include. EBRCSA also showed expenditures for the five items in the new agreement after it ends, as EBRCSA assumes these services will continue. EBRCSA is requesting the Committees to discuss the increased cost and recommend to the Board of Directors to direct the Executive Director to work with the Auditors Office on options concerning the cost increase.

RECOMMENDED ACTION:

It is requested that the Committees discuss and reach a consensus and make a recommendation to the Board concerning the proposed Motorola Agreement for ASTRO Maintenance, ASTRO SUA, MPLS, MDR, and NICE SUA and Maintenance.

Attachments:

“A” –Motorola Proposal SUA and Maintenance

“B” - FY 23/24 Approved Budget

“C” – FY 23/24 Amended Budget with Items Included

EAST BAY REGIONAL COMMUNICATIONS SYSTEM AUTHORITY

EBRCSA INFRASTRUCTURE SUA AND MAINTENANCE

JUNE 28, 2023

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

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2022 Motorola Solutions, Inc. All rights reserved.

Motorola Solutions, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781
USA

June 28, 2023

Mr. Tom McCarthy
Executive Director
EBRCSA
4985 Broder Blvd.
Dublin, CA 94568

Re: 6 Year SUA and Maintenance & Support Proposal

Dear Tom,

Motorola Solutions, Inc. ("Motorola") is pleased to submit to the East Bay Regional Communication System Authority (EBRCSA), the following Infrastructure Software Upgrade Agreement (SUA) and Maintenance and Support (M&S) proposal. This multi-year proposal outlines a cost-predictable path for comprehensive protection and refreshment of EBRCSA's mission critical communications infrastructure. The recommendations and delivery methodology proposed will align EBRCSA's ongoing upgrade and maintenance requirements with that of Motorola's product lifecycle for the next 6 years.

Motorola Solutions heavily invests in research and development to continually improve system capability, security and industry standards. Upgrading your network ensures you attain the most value from your investment with the latest features and security enhancements while reducing total cost of ownership. Through the SUA and Maintenance programs, you will extend the lifespan of your network with planned system updates, and receive the necessary upgrades, implementation and change management services required to maintain your network at the highest level of support.

Coverage in the proposal is multi-faceted and is intended not only for the ASTRO 25 system, but also key network elements interfacing with the ASTRO 25 system. This includes EBRCSA's MPLS network, as well as the audio recording infrastructure. The proposal encompasses upgrades through 2029, including costs for hardware, software, labor and technical resources required to execute the recommended upgrade and maintenance strategy.

The EBRCSA network is an indispensable component of public safety within Alameda and Contra Costa counties. Motorola has taken great care to propose a solution that ensures you will maintain critical network resiliency and security advancements in the most economically and financially sound manner possible.

This Proposal is a firm offer, subject to the terms and conditions of the existing Communications System Agreement (CSA) between EBRCSA and Motorola, dated July 07, 2009, as amended by Amendment No. 5 enclosed with the Proposal. EBRCSA may accept the proposal by delivering to Motorola a signed copy of Amendment No. 5 to the current CSA.

Motorola Solutions' proposal is conditional upon EBRCSA's acceptance of the terms and conditions included in this proposal, or a negotiated version thereof. Pricing will remain valid for 60 days from the date of this proposal.

Any questions EBRCSA has regarding this proposal can be directed to Michael Larson, Senior Account Manager at 530-333-7584, michael.larson@motorolasolutions.com.

Our goal is to provide EBRCSA with the best products and services available in the communications industry. We thank you for the trust you continue to have in Motorola and greatly appreciate the opportunity to continue to strengthen our long term relationship.

Thank you.

Regards,



Scott Lees
Vice President, Western Region
Motorola Solutions Inc.

TABLE OF CONTENTS

Section 1

ASTRO 25 Maintenance Services.....	1-1
1.1 Advanced Services Support Description.....	1-1
1.1.1 Overview	1-1
1.1.2 Advanced Services Element Descriptions.....	1-1
1.1.3 Network Event Monitoring.....	1-1
1.1.4 Remote Technical Support	1-1
1.1.5 Network Hardware Repair.....	1-2
1.1.6 Remote Security Update Service	1-2
1.1.7 On-site Infrastructure Response	1-2
1.1.8 Annual Preventive Maintenance	1-2
1.1.9 Managed Detection and Response.....	1-3
1.1.10 MPLS Maintenance and UEM Monitoring	1-3
1.1.11 Motorola Solutions Service Delivery Ecosystem	1-3
1.1.12 Centralized Managed Support Operations	1-3
1.1.13 Field Service	1-4
1.1.14 Repair Depot.....	1-4
1.1.15 Customer Support Manager.....	1-4
1.1.16 MyView Portal.....	1-4
1.2 ASTRO 25 Advanced Services Statement of Work.....	1-5
1.2.1 Overview	1-5
1.2.2 Motorola Solutions Service Delivery Ecosystem	1-6
1.2.3 Centralized Managed Support Operations	1-6
1.2.4 Field Service.....	1-7
1.2.5 Customer Support Manager.....	1-7
1.2.6 Repair Depot	1-7
1.2.7 MyView Portal.....	1-7
1.3 Connectivity Specifications	1-8
1.4 Advanced Services Detailed Description	1-8
1.4.1 Network Event Monitoring.....	1-8
1.4.1.1 Description of Service	1-9
1.4.1.2 Scope	1-10
1.4.1.3 Inclusions.....	1-10
1.4.1.4 Motorola Solutions Responsibilities.....	1-10
1.4.1.5 Limitations and Exclusions.....	1-10
1.4.1.6 Customer Responsibilities.....	1-11
1.4.1.7 Connectivity Matrix.....	1-12
1.4.1.8 Motorola Solutions Owned and Supplied Equipment.....	1-12
1.4.1.9 Monitored Elements	1-12



1.4.2	Remote Technical Support	1-13
1.4.2.1	Description of Service	1-13
1.4.2.2	Scope	1-14
1.4.2.3	Inclusions.....	1-14
1.4.2.4	Motorola Solutions Responsibilities.....	1-14
1.4.2.5	Limitations and Exclusions	1-15
1.4.2.6	Customer Responsibilities.....	1-15
1.4.3	Network Hardware Repair.....	1-15
1.4.3.1	Description of Service	1-15
1.4.3.2	Scope	1-16
1.4.3.3	Inclusions.....	1-16
1.4.3.4	Motorola Solutions Responsibilities.....	1-16
1.4.3.5	Limitations and Exclusions	1-17
1.4.3.6	Customer Responsibilities.....	1-17
1.4.3.7	Repair Process	1-19
1.4.4	Remote Security Update Service	1-20
1.4.4.1	Description of Service	1-20
1.4.4.2	Remote Update Requirements.....	1-20
1.4.4.3	Reboot Support.....	1-21
1.4.4.4	Scope	1-21
1.4.4.5	Inclusions.....	1-22
1.4.4.6	Motorola Solutions Responsibilities.....	1-22
1.4.4.7	Limitations and Exclusions	1-22
1.4.4.8	Customer Responsibilities.....	1-23
1.4.4.9	Reboot Responsibilities.....	1-23
1.4.4.10	Disclaimer	1-24
1.4.5	On-site Infrastructure Response	1-24
1.4.5.1	Description of Service	1-25
1.4.5.2	Scope	1-25
1.4.5.3	Inclusions.....	1-25
1.4.5.4	Motorola Solutions Responsibilities.....	1-25
1.4.5.5	Limitations and Exclusions	1-26
1.4.5.6	Customer Responsibilities.....	1-26
1.4.6	Annual Preventive Maintenance	1-27
1.4.6.1	Description of Service	1-27
1.4.6.2	Scope	1-27
1.4.6.3	Inclusions.....	1-28
1.4.6.4	Motorola Solutions Responsibilities.....	1-28
1.4.6.5	Limitations and Exclusions	1-28
1.4.6.6	Customer Responsibilities.....	1-29
1.4.6.7	Preventive Maintenance Tasks	1-29
1.5	Priority Level Definitions and Response Times.....	1-32

1.6	ASTRO 25 Managed Detection and Response.....	1-33
1.6.1	Summary.....	1-33
1.6.2	The ActiveEye SM Platform.....	1-33
1.6.3	Chief Information Security Officer (CISO) Benefits.....	1-34
1.6.4	Solution Overview.....	1-34
1.6.4.1	Site Information.....	1-35
1.6.5	Service Description.....	1-36
1.6.5.1	Managed Detection and Response Elements	1-36
1.6.5.2	Service Modules	1-40
1.6.5.3	Security Operations Center Services	1-41
1.7	MPLS Maintenance	1-41
1.8	NICE Gold Lite Maintenance Services.....	1-46
1.8.1	NICE SUA	1-46

Section 2

	Astro System Upgrade Agreement (SUA II) Statement Of Work	2-1
2.1	Overview	2-1
2.2	Scope	2-1
2.3	Inclusions	2-2
2.4	Limitations and Exclusions	2-2
2.4.1	Non-Standard Configurations	2-3
2.4.2	System Expansions and New Features	2-3
2.4.3	Security Update Service	2-3
2.5	System Upgrades.....	2-4
2.5.1	Upgrade Planning and Preparation.....	2-4
2.5.1.1	Motorola Solutions Responsibilities.....	2-4
2.5.1.2	Customer Responsibilities.....	2-4
2.5.2	System Readiness Checkpoint.....	2-5
2.5.2.1	Motorola Solutions Responsibilities.....	2-5
2.5.2.2	Customer Responsibilities.....	2-5
2.5.3	System Upgrade.....	2-6
2.5.3.1	Motorola Solutions Responsibilities.....	2-6
2.5.3.2	Customer Responsibilities.....	2-6
2.5.4	Upgrade Completion.....	2-6
2.5.4.1	Motorola Solutions Responsibilities.....	2-6
2.5.4.2	Customer Responsibilities.....	2-6
2.6	Special Provisions	2-6
2.7	ASTRO System Release Upgrade Paths.....	2-7

Section 3

	Managed Detection and Response Statement of Work.....	3-1
3.1	Overview	3-1
3.2	Description of Service.....	3-1



3.2.1	Deployment Timeline and Milestones	3-1
3.2.2	General Responsibilities	3-2
3.2.2.1	Motorola Solutions Responsibilities	3-2
3.2.2.2	Customer Responsibilities	3-2
3.2.3	Service Modules	3-3
3.2.3.1	Log Analytics	3-3
3.2.3.2	Network Detection	3-4
3.2.3.3	Vulnerability Detection	3-4
3.3	Security Operations Center Monitoring and Support	3-5
3.3.1	Scope	3-5
3.3.2	Ongoing Security Operations Center Service Responsibilities	3-5
3.3.3	Technical Support	3-6
3.3.4	Incident Response	3-6
3.3.5	Event Response and Notification	3-7
3.3.6	Priority Level Definitions and Notification Times	3-8

Section 4

Limitations and Exclusions	3-10
4.1.1 Service Limitations	3-10
4.1.2 Processing of Customer Data in the United States and/or other Locations	3-10
4.1.3 Customer and Third-Party Information	3-10
4.1.4 Third-Party Software and Service Providers, including Resale	3-11

Section 5

Pricing Summary	4-1
5.1 System Pricing Configuration	4-1
5.2 Infrastructure SUA and Maintenance Pricing	4-2
5.3 Maintenance and SUA Payment Terms	4-2
5.4 Managed Detection and response Payment Schedule & Terms	4-2

Section 6

Contractual Documentation	5-1
Amendment No. 5	5-1
to Communications System Agreement	5-1
Recitals	5-1
Agreement	5-2
Exhibit "A"	5-4
East Bay Regional Communications System Authority (EBRCSA) Infrastructure SUA and Maintenance Proposal dated June 28, 2023	5-4
Exhibit "B"	5-4
Maintenance, Support and Lifecycle Management Addendum	5-4
Exhibit "C"	5-9
Cyber Addendum	5-9
Exhibit "D"	5-17



Data Processing Addendum..... 5-17
Annex I..... 5-25
Annex II..... 5-30
Annex III..... 5-35

SECTION 1

ASTRO 25 MAINTENANCE SERVICES

1.1 ADVANCED SERVICES SUPPORT DESCRIPTION

1.1.1 Overview

Motorola Solutions is proposing our Advanced Services for ASTRO® 25 infrastructure, a comprehensive program to sustain the long-term performance of East Bay Regional Communications System Authority network. Advanced Services consists of the following elements:

- Network Event Monitoring.
- Remote Technical Support.
- Network Hardware Repair.
- Remote Security Update Service (RSUS).
- On-site Infrastructure Response.
- Annual Preventive Maintenance.
- Managed Detection and Response.
- MPLS Maintenance.
- NICE Gold Lite Maintenance Services.

Together, these elements will help to avoid operational disruptions and maintain the value of East Bay Regional Communications System Authority communications investment.

1.1.2 Advanced Services Element Descriptions

The following sections describe the elements proposed for East Bay Regional Communications System Authority ASTRO 25 infrastructure.

1.1.3 Network Event Monitoring

Motorola Solutions will continuously monitor East Bay Regional Communications System Authority ASTRO 25 network to detect potential issues or communications outages, maximizing network uptime. Motorola Solutions assesses each alert with advanced event detection and correlation algorithms to determine how to respond. Potential responses include remote restoration or dispatching a local field technician to resolve the incident on-site.

1.1.4 Remote Technical Support

Motorola Solutions' Centralized Managed Support Operations (CMSO) will provide Remote Technical Support for infrastructure issues that require specific technical expertise. Experienced technical support specialists will be available to consult with EBRCSA to help



diagnose, troubleshoot, and resolve infrastructure issues. Service Desk maintenance procedures and incident resolution techniques are based on ISO 9001 and TL 9000 standards.

1.1.5 Network Hardware Repair

To restore East Bay Regional Communications System Authority ASTRO 25 network components if they malfunction, Motorola Solutions will repair Motorola Solutions-provided infrastructure equipment. This includes select third-party infrastructure equipment supplied by Motorola Solutions. Motorola Solutions will ship and return repaired equipment, and will coordinate the repair of third-party solution components.

1.1.6 Remote Security Update Service

Commercial security software updates are often designed without consideration for specialized systems like radio communications networks. These updates may inadvertently disrupt ASTRO 25 network operations and functionality.

To minimize cyber risks and software conflicts, Motorola Solutions provides the Remote Security Update Service (RSUS). With this service, Motorola Solutions deploys antivirus and operating system security updates on an ASTRO 25 network in a dedicated information assurance lab to test and validate them for use with ASTRO 25 networks.

Motorola Solutions tests whether applying these security updates degrades network service. If an update degrades performance, Motorola Solutions searches for a solution or workaround to address the issue before releasing that update.

With RSUS, Motorola Solutions will remotely install tested updates on East Bay Regional Communications System Authority ASTRO 25 network. If there are any recommended configuration changes, warnings, or workarounds, Motorola Solutions will provide detailed documentation on a secured extranet website.

1.1.7 On-site Infrastructure Response

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

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

1.1.8 Annual Preventive Maintenance

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

1.1.9 Managed Detection and Response

Experienced, specialized cybersecurity analyst at Motorola Solutions' Security Operations Center (SOC) will monitor Customer's ASTRO 25 radio network and Customer Enterprise Network (CEN) 24/7/365 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.

1.1.10 MPLS Maintenance and UEM Monitoring

Motorola Solutions is in the process of adding the MPLS routers to the ASTRO Network Management platform UEM. Motorola will monitor the UEM for alarms. Real-time, continuous "endpoint" event monitoring of the MPLS backhaul network components, directing the Customer's attention to potential disruptions to backhaul connections.

1.1.11 Motorola Solutions Service Delivery Ecosystem

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

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

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

1.1.12 Centralized Managed Support Operations

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

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

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

1.1.13 Field Service

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

1.1.14 Repair Depot

The Motorola Solutions Repair Depot will provide EBRCSA with a central repair location. This will eliminate the need to send network equipment to multiple vendor locations for repair. Motorola Solutions tracks products sent to the Depot via a case management system throughout the repair process. This system will enable East Bay Regional Communications System Authority representatives to check repair status, from inbound shipment to return.

1.1.15 Customer Support Manager

A Motorola Solutions Customer Support Manager (CSM) will be East Bay Regional Communications System Authority key point of contact for the definition and administration of services. The CSM will work with EBRCSA to define service delivery details to address East Bay Regional Communications System Authority specific priorities.

1.1.16 MyView Portal

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



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

With MyView Portal, East Bay Regional Communications System Authority administrators will be able to monitor system health and maintenance updates. Capabilities include:

- Viewing network and support compliance.

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

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

1.2 ASTRO 25 ADVANCED SERVICES STATEMENT OF WORK

1.2.1 Overview

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

Advanced Services consist of the following elements:

- Network Event Monitoring.
- Remote Technical Support.
- Network Hardware Repair.
- Remote Security Update Service.
- On-site Infrastructure Response.
- Annual Preventive Maintenance.
- Managed Detection and Response.
- MPLS Maintenance.
- NICE Gold Lite Maintenance Services.

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

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

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

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 Solutions 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.



Remote Technical Support

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

Network Hardware Repair

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

Remote Security Update Service

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

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.

Managed Detection and Response

Real-time, continuous ASTRO 25 radio network security elements monitoring by specialized security technologists with extensive experience working with ASTRO 25 mission-critical networks.

1.2.2 Motorola Solutions Service Delivery Ecosystem

Advanced 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 MyView Portal. 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.

1.2.3 Centralized Managed Support Operations

The cornerstone of Motorola Solutions' support process is the Centralized Managed Support Operations ("CMSO") organization, which includes the Service Desk and technical support teams. The CMSO is staffed 24x7x365 by experienced personnel, including service desk specialists, security analysts, and operations managers.

The Service Desk provides a single point of contact for all service related items, including communications between the Customer, Motorola Solutions, and third-party subcontractors. The Service Desk processes service requests, service incidents, change requests, and



dispatching, and communicates with stakeholders in accordance with pre-defined response times.

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

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

1.2.4 Field Service

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

1.2.5 Customer Support Manager

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

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

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

1.2.6 Repair Depot

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

1.2.7 MyView Portal

Supplementing the CSM and the Service Desk as the Customer points of contact, MyView Portal 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 Solutions’ repair depot and eliminate the need to call for status updates. In certain countries, customers will also have the ability to create new RMA requests online.
- Remote Security Update Service: View patch history and status of recently completed security updates.
- 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.
- Security Monitoring: 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 MyView Portal 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

The Advanced Services package requires available internet connectivity provided by the Customer. A minimum connection of 2 Mbps is necessary to enable remote monitoring and update services.

1.4 ADVANCED 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 Network Event Monitoring

Network Event Monitoring provides continuous real-time fault monitoring for radio communications networks. Motorola Solutions 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. Centralized Managed Support Operations (“CMSO”) technologists acknowledge and assess these incidents, and initiate a defined response.



1.4.1.1 Description of Service

With Network Event Monitoring, Motorola Solutions 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 1-1: Alarm Threshold Rule Options for all Event Types.

Table 1-1: 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 Solutions’ response may include continued monitoring for further incident development, remote remediation by technical support, dispatching a field service technician, or other actions Motorola Solutions determines necessary.

To prevent duplicate incidents from being generated by the same root cause, Motorola Solutions 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 Solutions 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 Solutions and the Customer can reference these templates. When information is updated, it will be organized in four categories:

- Open: – Motorola Solutions’ 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 MyView Portal, including incident management reports. Any specific remediation and action notes from Motorola Solutions’ 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 MyView Portal, 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 Solutions make 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 Scope

Network Event Monitoring is available 24 hours a day, 7 days a week. Incidents generated by the monitoring service will be handled in accordance with Section 1.5 Priority Level Definition 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.

1.4.1.3 Inclusions

Network Event Monitoring is available for the devices listed in Section 1.4.1.9 Monitored Elements.

1.4.1.4 Motorola Solutions Responsibilities

- Provide a dedicated network connection necessary for monitoring the Customer's communication network. Section 1.4.1.7 Connectivity Matrix describes available connectivity options.
- If determined necessary by Motorola Solutions, provide Motorola Solutions-owned equipment at the Customer's premises for monitoring network elements. The type of equipment and location of deployment is listed in Section 1.4.1.8 Motorola Solutions Owned and Supplied Equipment.
- Verify connectivity and event monitoring prior to system acceptance or start date.
- Monitor system continuously during hours designated in the Customer Support Plan ("CSP"), and in accordance with Section 1.5 Priority Level Definitions and Response Times.
- Remotely access the Customer's system to perform remote diagnosis as permitted by the Customer pursuant to Section 1.4.1.6 Customer Responsibilities.
- Create an incident, as necessary. Gather information to perform the following:
 - Characterize the issue.
 - Determine a plan of action.
 - Assign and track the incident to resolution.
- Provide the Customer with a link to access system configuration info, site info, system notifications, and system notes.
- Cooperate with the Customer to coordinate the transition of monitoring responsibilities between Motorola Solutions and the Customer as specified in Section 1.4.1.6 Customer Responsibilities.
- If the Customer's technician designated in the CSP is Mobile OSS ("MOSS") enabled, the incident will be Automatically Dispatched to MOSS. Otherwise, the incident will be sent to the CMSO Service Desk.
- Maintain communication as needed with the Customer in the field until incident resolution.
- Provide available information on incident resolution to the Customer.

1.4.1.5 Limitations and Exclusions

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

- Motorola Solutions 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 Solutions determines that system faults were caused by the Customer making changes to critical system parameters without written agreement from Motorola Solutions.
- Monitoring of network transport, such as WAN ports, WAN cloud, and redundant paths, unless provided by supplemental service outside this standard scope.

1.4.1.6 Customer Responsibilities

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

is transferring monitoring from Motorola Solutions for network monitoring after normal business hours.

- Upon contact, the Customer must provide Motorola Solutions with customer name, site ID, status on any open incidents, priority level of any open incidents, brief descriptions of any ongoing incident, and action plan for resolving those incidents.
- Acknowledge that incidents will be handled in accordance with Section 1.5 Priority Level Definitions and Response Times.

1.4.1.7 Connectivity Matrix

Request connectivity eight weeks in advance of service start date.

Table 1-2: Available Connectivity

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

1.4.1.8 Motorola Solutions Owned and Supplied Equipment

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

Table 1-3: Motorola Solutions Owned and Supplied Equipment

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

1.4.1.9 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 is inventoried in section 4.1 System Pricing Configuration.

Table 1-4: Monitored Elements

Monitored Elements		
Active Directory	Enrichment Testing	Probe
Agent	Environmental	Radio Interface
AIS	ESX	RDM
AMB	Exit Router	RFDS
Application Server	Firewall	RGU
APX Cloud Application	GAS Server	RNG
ATR	Gateway	Router
AUC	Gateway Router	RTU
Backup Server	Gateway Unit	Short Data Router
Base Radio	HSS	Site

Call Processor	Infrastructure (CHI CAM)	Statistical Server
CAM	Install Server	Storage Networking
CBSD	LAN Switch	Switch
CCGW	Licensing Service	Telephony
Channel	Link	Terminal Server
Client Station	Load Balancer	Time Keeper
CommandCentral AXS dispatch console	Logging Recorder	Training App
Controller	Logging Replay Station	Training Database
Conventional	MME	TRAK
Core	MOSCAD Server	Trap Forwarder
Core Router	Network Address	UCS
Data Processing	Network Device	UEM
Database Server	NTP	Virtual Machine
Data Warehouse Server	OP	VMS
Device Configuration Server	OSP	VPM
DNS	Packet Data Gateway	WSGU
Domain Controller	Physical Host Environmental	ZDS
DSC 8000 Site Controller	Physical Host Power and Network	Zone Controller
eNodeB	Power Distribution Unit	-

1.4.2 Remote Technical Support

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

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

1.4.2.1 Description of Service

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

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

The CMSO Operations Center classifies and responds to each technical support request in accordance with Section 1.5 Priority Level Definitions and Response Times.

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

1.4.2.2 Scope

The CMSO Service Desk is available via telephone 24 hours per day, 7 days per week, and 365 days per year to receive and log requests for technical support. Remote Technical Support service is provided in accordance with Section 1.5 Priority Level Definitions and Response Times.

1.4.2.3 Inclusions

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

1.4.2.4 Motorola Solutions Responsibilities

- Maintain availability of the Motorola Solutions CMSO Service Desk via telephone (800-MSI-HELP) 24 hours per day, 7 days per week, and 365 days per year to receive, log, and classify Customer requests for support.
- Respond to incidents and technical service requests in accordance with Section 1.5 Priority Level Definitions and Response Times.
- Provide caller a plan of action outlining additional requirements, activities, or information required to achieve restoral/fulfillment.
- Maintain communication with the Customer in the field as needed until resolution of the incident.
- Coordinate technical resolutions with agreed upon third-party vendors, as needed.
- Escalate support issues to additional Motorola Solutions technical resources, as applicable.
- Determine, in its sole discretion, when an incident requires more than the Remote Technical Support services described in this SOW and notify the Customer of an alternative course of action.



1.4.2.5 Limitations and Exclusions

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

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

1.4.2.6 Customer Responsibilities

- Prior to contract start date, provide Motorola Solutions with pre-defined information necessary to complete Customer Support Plan (“CSP”).
- Submit timely changes in any information supplied in the CSP to the Customer Support Manager (“CSM”).
- Contact the CMSO Service Desk to engage the Remote Technical Support service when needed, providing the necessary information for proper entitlement services. This information includes, but is not limited to, the name of contact, name of Customer, system ID number, site(s) in question, and a brief description of the problem that contains pertinent information for initial issue classification.
- Maintain suitably trained technical resources familiar with the operation of the Customer’s system to provide field maintenance and technical maintenance services for the system.
- Supply suitably skilled and trained on-site presence when requested.
- Validate issue resolution in a timely manner prior to close of the incident.
- Acknowledge that incidents will be addressed in accordance with Section 1.5 Priority Level Definitions and Response Times.
- Cooperate with Motorola Solutions, and perform all acts that are reasonable or necessary to enable Motorola Solutions to provide Remote Technical Support.
- In the event that Motorola Solutions agrees in writing to provide supplemental Remote Technical Support to third-party elements provided by the Customer, the Customer agrees to obtain all third-party consents or licenses required to enable Motorola Solutions to provide the service.

1.4.3 Network Hardware Repair

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

1.4.3.1 Description of Service

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



Network Hardware Repair is also known as Infrastructure Repair.

1.4.3.2 Scope

Repair authorizations are obtained by contacting the Centralized Managed Support Operations (“CMSO”) organization Service Desk, which is available 24 hours a day, 7 days a week. Repair authorizations can also be obtained by contacting the Customer Support Manager (“CSM”).

1.4.3.3 Inclusions

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

1.4.3.4 Motorola Solutions Responsibilities

- Provide the Customer access to the CMSO Service Desk, operational 24 hours a day and 7 days per week, to request repair service.
- Provide repair return authorization numbers when requested by the Customer.
- Receive malfunctioning infrastructure components from the Customer and document its arrival, repair, and return.
- Conduct the following services for Motorola Solutions infrastructure:
 - Perform an operational check on infrastructure components to determine the nature of the problem.
 - Replace malfunctioning components.
 - Verify that Motorola Solutions infrastructure components are returned to applicable Motorola Solutions factory specifications.
 - Perform a box unit test on serviced infrastructure components.
 - Perform a system test on select infrastructure components.
- Conduct the following services for select third-party infrastructure:
 - When applicable, perform pre-diagnostic and repair services to confirm infrastructure component malfunctions and prevent sending infrastructure components with No Trouble Found (“NTF”) to third-party vendor for repair.
 - When applicable, ship malfunctioning infrastructure components to the original equipment manufacturer or third-party vendor for repair service.
 - Track infrastructure components sent to the original equipment manufacturer or third-party vendor for service.
 - When applicable, perform a post-test after repair by original equipment manufacturer or third-party vendor to confirm malfunctioning infrastructure components have been repaired and function properly in a Motorola Solutions system configuration.
- Reprogram repaired infrastructure components to original operating parameters based on software and firmware provided by the Customer, as required in Section 1.4.3.6 Customer Responsibilities. If the Customer’s software version and configuration are not provided, shipping will be delayed. If the repair depot determines that infrastructure components are malfunctioning due to a software



defect, the repair depot reserves the right to reload these components with a different but equivalent software version.

- Properly package repaired infrastructure components.
- Ship repaired infrastructure components to Customer-specified address during normal operating hours of Monday through Friday from 7:00 a.m. to 7:00 p.m. Central Standard Time (“CST”), excluding holidays. Infrastructure component will be sent using two-day air shipping unless the Customer requests otherwise. Motorola Solutions will pay for shipping unless the Customer requests shipments outside of the above mentioned standard business hours or carrier programs, such as next flight out (“NFO”). In such cases, the Customer will be responsible for paying shipping and handling charges.

1.4.3.5 Limitations and Exclusions

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

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

1.4.3.6 Customer Responsibilities

- Contact or instruct servicer to contact the Motorola Solutions CMSO organization, and request a return authorization number prior to shipping malfunctioning infrastructure components.
- Provide model description, model number, serial number, type of system, software and firmware version, symptom of problem, and address of site location for spare infrastructure components.



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



1.4.3.7 Repair Process

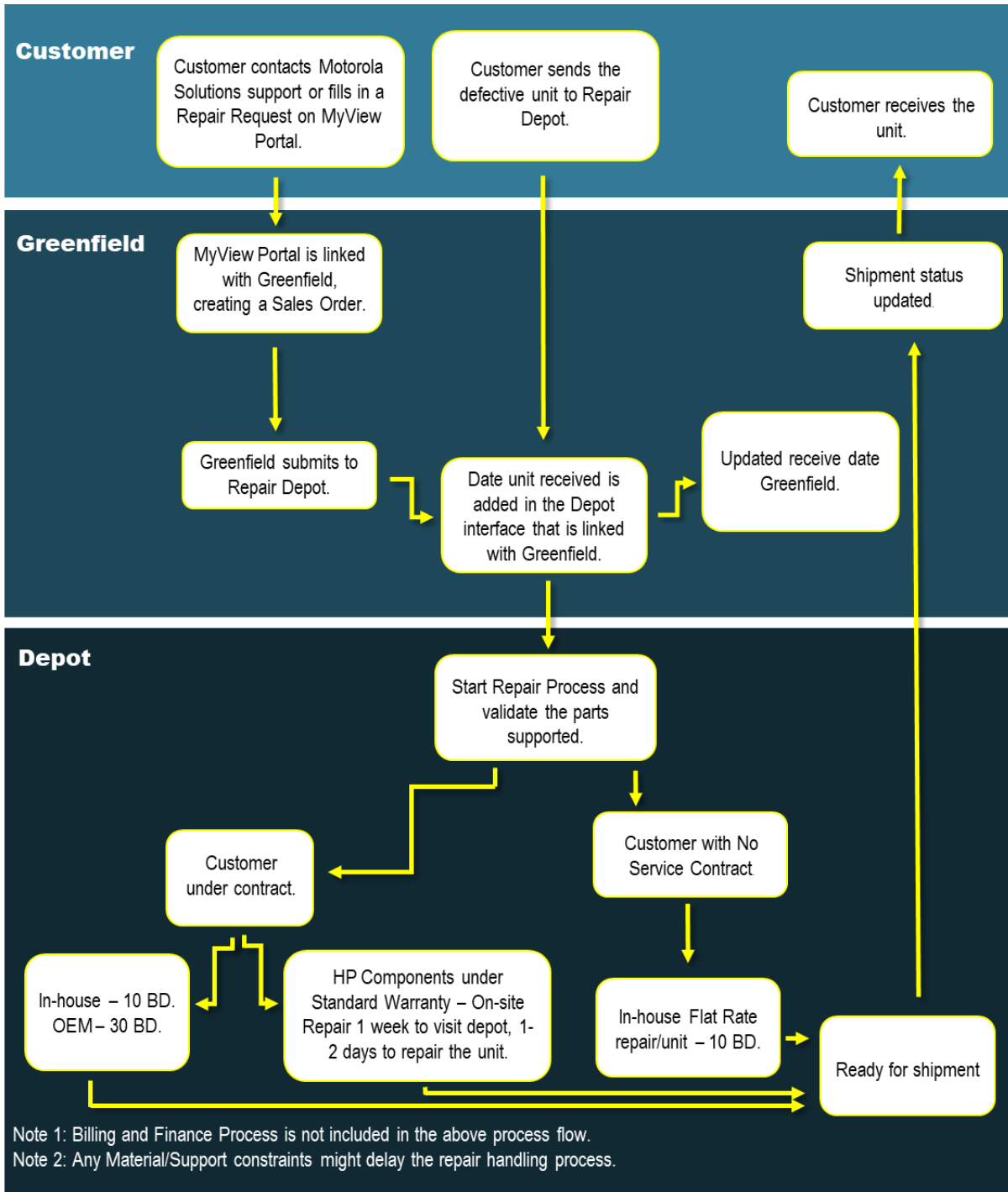


Figure 1-2: Repair Decision Process

1.4.4 Remote Security Update Service

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

The ASTRO 25 Security Update Service ("SUS") and Network Event Monitoring service are prerequisites for RSUS. These prerequisites are included as part of this service package.

1.4.4.1 Description of Service

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

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

1.4.4.2 Remote Update Requirements

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

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

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



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

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

1.4.4.3 Reboot Support

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

1.4.4.4 Scope

RSUS includes pretested security updates for the software listed in Table 1-5: Update Cadence. This table also describes the release cadence for security updates.

Table 1-5: Update Cadence

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

Motorola Solutions installs security updates during normal business hours. Normal business hours are defined as 8 a.m. to 5 p.m. Central Standard Time on Monday through Friday, excluding Public Holidays. The Customer may submit a formal request that Motorola Solutions personnel work outside of these hours. The Customer may need to pay additional costs for work to be completed outside of normal business hours.

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

Intrusive security updates require Customer coordination, may require hardware reboots and zone controller rolling (switching from one zone controller to the other) to fully implement. Systems with redundant zone controllers (L2, M2, M3) have low downtime (minutes) as the zone controllers are rolled, but systems with single zone

controllers (L1, M1) will be down for longer periods. While rolling the zone controllers, the system will operate in “Site trunking” mode. The Customer will need to be aware of these operational impacts, and coordinate events with users.

1.4.4.5 Inclusions

Supported ASTRO 25 core types and security update delivery methods are included in Table 1-6: SUS Packages. This table indicates if Motorola Solutions will provide any RSUS optional services to the Customer. RSUS supports the current Motorola Solutions ASTRO 25 system release and aligns with the established [Software Support Policy \(SwSP\)](#).

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

Table 1-6: SUS Packages

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	X

Responsibilities for rebooting applicable hardware are detailed in Section 1.4.4.9 Reboot Responsibilities.

1.4.4.6 Motorola Solutions Responsibilities

- If required, in order to provide the services, Motorola Solutions will send to the customer a secure router and / or a Network Management Client for installation in the ASTRO system. If the Customer is unable to install, please contact your CSM who will be able to arrange for this to be completed.
- Remotely deploy upatches listed in Section 1.4.4.4 Scope on the Customer’s system. Patches will be installed on the cadence described in that section.
 - As outlined in Section 1.4.4.4 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 no security updates are released by the OEMs during the usual time period, Motorola Solutions will send a notice that no new security updates were deployed.

1.4.4.7 Limitations and Exclusions

- Systems with non-standard configurations that have not been certified by Motorola Solutions’ Systems Integration and Test (“SIT”) team are specifically



excluded from this service, unless otherwise agreed in writing by Motorola Solutions.

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

1.4.4.8 Customer Responsibilities

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

1.4.4.9 Reboot Responsibilities

Motorola Solutions will provide reboot services only for the core. 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 1-7: Reboot Responsibilities Matrix contains the breakdown of responsibilities. Section 1.4.4.5 Inclusions indicates which services are included.



Table 1-7: Reboot Responsibilities Matrix

Remote SUS Package	Motorola Solutions Responsibilities	Customer Responsibilities
Remote Security Update Service	Provide a report to the Customer's main contact listing the servers or workstations for the core 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 Solutions.
Remote Security Update Service with Reboot Support	When a security update requires a reboot, dispatch a technician to reboot servers and workstations for the core after security updates are installed.	

1.4.4.10 Disclaimer

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

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

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

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

1.4.5 On-site Infrastructure Response

Motorola Solutions' On-site Infrastructure Response service provides incident management and escalation for on-site technical service requests. The service is delivered by Motorola Solutions' Centralized Managed Support Operations ("CMSO") organization in cooperation with a local service provider. The following includes the equipment covered:

- Master Site including the Master Site CEN



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

1.4.5.1 Description of Service

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

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

The dispatched field service technician will travel to the Customer's location to restore the system in accordance with Section 1.5 Priority Level Definitions and Response Times.

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

1.4.5.2 Scope

On-site Infrastructure Response is available 24 hours a day, 7 days a week in accordance with Section 1.5 **Error! Reference source not found.** Customer's Response Time Classification is designated in the Customer Support Plan.

1.4.5.3 Inclusions

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

1.4.5.4 Motorola Solutions Responsibilities

- Receive service requests.
- Create an incident when service requests are received. Gather information to characterize the issue, determine a plan of action, and assign and track the incident to resolution.
- Dispatch a field service technician, as required by Motorola Solutions' standard procedures, and provide necessary incident information.
- Provide the required personnel access to relevant Customer information, as needed.
- Motorola Solutions field service technician will perform the following on-site:
 - Run diagnostics on the infrastructure component.
 - Replace defective infrastructure component, 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 Customer Support Plan ("CSP"), verify with the Customer that restoration is complete or system is



functional. If verification by the Customer cannot be completed within 20 minutes of restoration, the incident will be closed and the field service technician will be released.

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

1.4.5.5 Limitations and Exclusions

The following items are excluded from this service:

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

1.4.5.6 Customer Responsibilities

- Contact Motorola Solutions, as necessary, to request service.
- Prior to start date, provide Motorola Solutions with the following pre-defined Customer information and preferences necessary to complete CSP:
 - Incident notification preferences and procedure.
 - Repair verification preference and procedure.
 - Database and escalation procedure forms.



- Submit timely changes in any information supplied in the CSP to the Customer Support Manager (“CSM”).
- Provide the following information when initiating a service request:
 - Assigned system ID number.
 - Problem description and site location.
 - Other pertinent information requested by Motorola Solutions to open an incident.
- Provide field service technician with access to equipment.
- Supply infrastructure spare or FRU, as applicable, in order for Motorola Solutions to restore the system.
- Maintain and store software needed to restore the system in an easily accessible location.
- Maintain and store proper system backups in an easily accessible location.
- If required by repair verification preference provided by the Customer, verify with the CMSO Service Desk and dispatch that restoration is complete or system is functional.
- Cooperate with Motorola Solutions and perform reasonable or necessary acts to enable Motorola Solutions to provide these services.
- In the event that Motorola Solutions agrees in writing to provide supplemental On-site Infrastructure Response to Customer-provided third-party elements, the Customer agrees to obtain and provide applicable third-party consents or licenses to enable Motorola Solutions to provide the service.

1.4.6 Annual Preventive Maintenance

Motorola Solutions personnel will perform a series of maintenance tasks to keep network equipment functioning correctly. The following includes the equipment covered:

- Master Site including the Master Site CEN
- Prime Site Controllers

1.4.6.1 Description of Service

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

1.4.6.2 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.



1.4.6.3 Inclusions

Annual Preventive Maintenance service will be delivered for Motorola Solutions-provided infrastructure, including integrated third-party products, per the level of service marked in Table 1-8: Preventive Maintenance Level.

Table 1-8: Preventive Maintenance Level

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

1.4.6.4 Motorola Solutions Responsibilities

- Notify the Customer of any planned system downtime needed to perform this service.
- Maintain communication with the Customer as needed until completion of the Annual Preventive Maintenance.
- Determine, in its sole discretion, when an incident requires more than the Annual Preventive Maintenance services described in this SOW, and notify the Customer of an alternative course of action.
- Provide the Customer with a report in MyView Portal, or as otherwise agreed in the Customer Support Plan (“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 1.4.6.7 Preventative Maintenance Tasks.
 - Perform the procedures defined in Section **Error! Reference source not found.** 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.

1.4.6.5 Limitations and Exclusions

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

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



1.4.6.6 Customer Responsibilities

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

1.4.6.7 Preventive 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 1.4.6.3: Inclusions.

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

MASTER 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 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 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.

PRIME SITE CHECKLIST – LEVEL 1	
Software	
Verify System software physical media	Perform audit of software media on site. Verify that versions, KC numbers, and types match what is deployed to Customer server.
Switches	
Equipment Alarms	Check LED and/or other status indicators for fault conditions.
Capture Diagnostics	Perform recommended diagnostic tests based on switch type. Capture available diagnostic logs.
Clean Fans and Equipment	Use antistatic vacuum to clean cooling pathways.

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

1.5 PRIORITY LEVEL DEFINITIONS AND RESPONSE TIMES

Table 1-9: Priority Level Definitions and Response Times describes the criteria Motorola Solutions uses to prioritize incidents and service requests, and lists the response times for those priority levels.

Table 1-9: Priority Level Definitions and Response Times

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



Incident Priority	Incident Definition	Initial Response Time	On-site Response Time
Medium P3	<p>Consoles: Up to 20% of a site's console positions down.</p> <p>Conventional Channels: Single channel down. Redundant gateway available.</p> <p>Network Elements: Site router/switch or GPS server down. Redundant networking element available.</p>	<p>Response provided during normal business hours until service restoration.</p> <p>Technical resource will acknowledge incident and respond within 4 hours of CMSO logging incident.</p>	<p>Response provided during normal business hours until service restoration.</p> <p>Field service technician arrival on-site within 8 hours of receiving dispatch notification.</p>
Low P4	<p>Service Requests: Minor events and warnings in the system. Preventative and planned maintenance activities (scheduled work).</p>	<p>Response provided during normal business hours.</p> <p>Motorola Solutions will acknowledge and respond within 1 Business Day.</p>	Not applicable.

1.6 ASTRO 25 MANAGED DETECTION AND RESPONSE

1.6.1 Summary

Motorola Solutions' ASTRO 25 MDR provides radio network security element monitoring by experienced, specialized security technologists with extensive experience working with ASTRO 25 mission-critical networks. For highly complex or unusual security events, Motorola Solutions' technologists have direct access to Motorola Solutions engineers for rapid resolution.

Our solution provides 24x7x365 Security Operations Center Support. This is a component of our broader proprietary SOC 2 Type 2 certified Managed Security Platform targeted to Public Safety, Critical Infrastructure, and State/Local municipalities.

1.6.2 The ActiveEyeSM Platform

In 2020, Motorola Solutions acquired Delta Risk, a leading Managed Security Services Provider (MSSP). The acquisition now allows Motorola Solutions to extend the ActiveEye platform to our customers and deliver a co-managed approach to 24/7 security monitoring operations across IT enterprise environments. The benefits of the ActiveEye platform are demonstrated below:

- Included Public Safety Threat Data Feed — Threat reports covering potential attack vectors based on dark web research. Summaries of actual attacks against public safety and state/local municipalities. Indicator data pulled from a large network of deployed public safety sensors and state/local municipality environments.
- Advanced Threat Detection & Response — Consolidate SIEM data and direct threat inputs from endpoint security, network sensors, and cloud/SaaS applications. Pre-built custom playbooks to process alerts and reduce/eliminate manual analyst effort.



- Single Dashboard for Threat Visibility — Prioritize based on actual assets in the environment. Asset inventory created manually or automatically with Managed Vulnerability Assessment Service - external and authenticated scans of assets, providing a complete attack surface map.

1.6.3 Chief Information Security Officer (CISO) Benefits

Main dashboard displays and aggregates all of the important and relevant risk information from across the organization, helping decision makers to make better-informed decisions to balance cybersecurity efforts and operational efficiencies.

Main dashboard provides key performance metrics and indicators that can inform an admin at a glance to the activity that is occurring throughout their environment.

Create ad-hoc reports and notifications based on available data and ActiveEye parameters.

Transparency into the service that Motorola Solutions is providing. The dashboard will provide the key indicators to the number of events that are handled on a daily, weekly, monthly basis and how those events are handled by the Motorola Solutions Security Operations Center (SOC).

Public Safety Threat Alliance

Cyber threats to public safety agencies are increasing in scope, scale, and complexity; however, most agencies lack the cybersecurity capabilities required to mitigate risk and ensure continuity of public safety operations. To address this critical need, Motorola Solutions has established a cyber threat information sharing and analysis organization (ISAO) for public safety called The Public Safety Threat Alliance (PSTA). The PSTA is recognized by the U.S. Cybersecurity and Infrastructure Security Association (CISA), and highlights Motorola Solutions' commitment to public safety agencies and the communities they serve.

The PSTA will leverage cybersecurity risk information from across Motorola Solutions' Cybersecurity Services. This, paired with information from members and trusted partners including CISA, other ISAOs, and nonprofits dedicated to sharing cyber threat intelligence, will help generate actionable intelligence to improve members' cybersecurity posture, defense, and resilience against evolving threats to their public safety missions. Membership in the PSTA is open to all public safety agencies. While initial efforts are focused on U.S. public safety, the Alliance will include global public safety agencies in the future.

Learn more about the Public Safety Threat Alliance at:
<https://motorolasolutions.com/public-safety-threat-alliance>.

1.6.4 Solution Overview

Motorola Solutions, Inc. (Motorola Solutions) is pleased to present the proposed cybersecurity services for East Bay Regional Communications System Authority (hereinafter referred to as "Customer").

Identifying and mitigating cyber threats requires a reliable solution that supplies the right data to cybersecurity experts. With MDR, Motorola Solutions will provide access to our

ActiveEyeSM Security Platform, along with 24x7 support from specialized security technologists, who will monitor your mission critical network against threat and intrusion.

The following ASTRO[®] 25 Managed Detection and Response features and services are included in our proposal:

- **ActiveEyeSM Managed Detection and Response Elements.**
 - ActiveEye Security Management Platform
 - ActiveEye Remote Security Sensor (AERSS)
 - Internetworking Firewall
- **Service Modules**
 - Log Collection / Analytics
 - Network Detection
 - Vulnerability Detection
- **Security Operations Center Monitoring and Support**

1.6.4.1 Site Information

The following site information is included in the scope of our proposal:

Table 1-10. Site Information

Site / Location	Quantity
Core Site	1
Control Room CEN	2
Co-located CEN	1
Network Management Clients	3
Dispatch Consoles	223
AIS	8
CEN Endpoints	10

Services Included

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

Table 1-11: Service Modules

Service Module	Features Included	Network Environment	Subscribed
ActiveEye Remote Security Sensor (AERSS)	Number of sensors: 4 <ul style="list-style-type: none"> • (3) CEN • (1) Core Site 	RNI CEN	X

Service Module	Features Included	Network Environment	Subscribed
Log Collection / Analytics	Online Storage Period: 30 Day Storage Extended Log Storage Length: 12 Months	RNI CEN	X
Network Detection	Up to 1 Gbps per sensor port	RNI CEN	X
Vulnerability Detection	Vulnerability Scanning Endpoints	Control Room CEN	X

The following table lists any ancillary components included.

Table 1-12. Ancillary Components

Description	Quantity
Internetworking Firewall	1

1.6.5 Service Description

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

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

The Managed Detection and Response service includes the deployment and optimization of these elements into the Customer’s network.

1.6.5.1 Managed Detection and Response Elements

This section and its subsections describe Managed Detection and Response elements, and their applicability for specific infrastructure.

1.6.5.1.1 ActiveEye Security Platform

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



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

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

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

1.6.5.1.2 ActiveEye Managed Security Portal

The ActiveEye Managed Security Portal will synchronize security efforts between the Customer and Motorola Solutions. From this central point, the Customer will be able to view threat insights, event investigations, security reports, threat advisories, and status of any security cases.

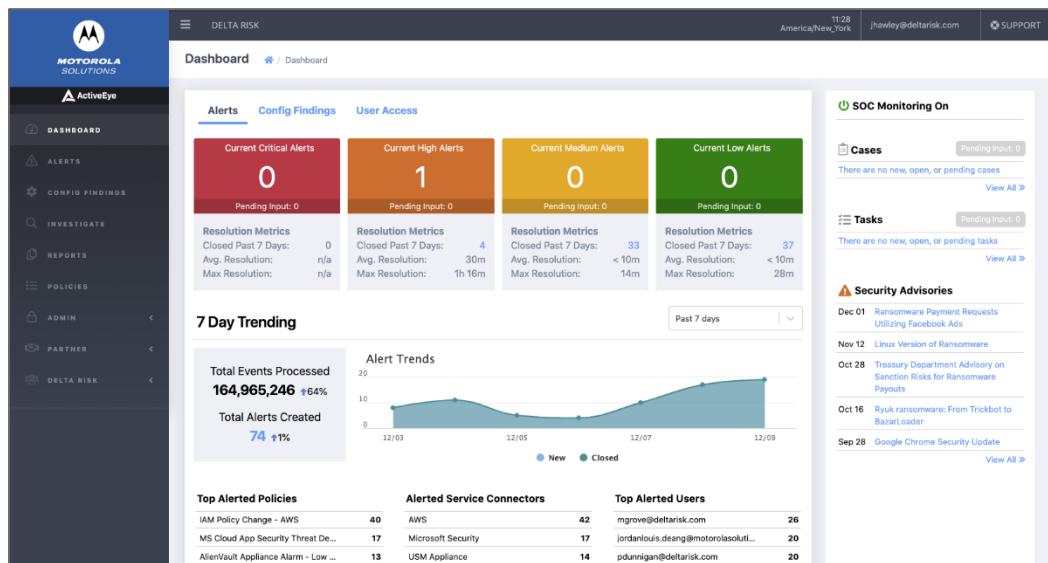


Figure 1-3: ActiveEye Interface

Dashboard

Key information in the ActiveEye Portal is summarized on the dashboard. This dashboard provides details about open alerts, an overview of alert categories, alert processing, key performance indicators (KPI), open security cases, and recent threat advisories. Also, users can access more in-depth information like security cases, alert details, alert trends, reports, and group communications.

Security Cases

When the Customer and Motorola Solutions identify a threat, the SOC will create a security case. Through the ActiveEye Portal, the Customer can view details of current or past cases, create new cases, or respond to ongoing cases.

Alert Details and Trends

Alerts can be evidence of a past, active, or developing threat. ActiveEye records relevant data for each alert, enabling users to quickly view its triggers, systems it impacts, and any actions taken to address the alert. ActiveEye Portal also provides tools for reviewing groups of alerts based on key attributes or time periods. Attribute filters enable users to toggle which alert groups ActiveEye Portal shows, helping to spot trends or threat activity. Users can also compare alert logs for specific time periods to determine if specific trends are associated with a threat or are false positives.

Investigations and Reporting

ActiveEye Portal includes robust *ad hoc* reporting capabilities, which will provide important, additional information about active and historical threats. Users can share information outside of ActiveEye Portal by downloading reports in .csv or .json format.

In addition to *ad hoc* reporting, ActiveEye Portal can provide a daily email summary and monthly report. Daily email summaries can include alert counts, security cases opened or closed, saved queries that have new data, and detailed endpoint security statistics. If needed, ActiveEye Portal can send one or more summary emails with different content for different groups. Monthly reports are available as a PDF download.

Security Advisories

Security Advisories are messages initiated from the SOC that share information on active threats with the Customer's security teams. These advisories guide security teams on how to best take action against a threat and tell them where they can find further information.

Information Sharing

The ActiveEye Portal includes several functions for sharing information. Automatic security alerts notify pre-defined contacts of incidents, based on incident priority. Other information sharing functions include:

- **SOC Bulletins** - Instructions from the Customer, or the SOC, that SOC analysts reference when creating security cases. These can communicate short-term situations where a security case may not be needed, such as during testing or maintenance windows.
- **Customer Notebook** - The SOC will use the Customer Notebook to document the Customer's environment and any specific network implementation details that will help the SOC investigate security cases.
- **Contact Procedures** - Escalation procedures and instructions on who to contact if an incident occurs. Contact procedures include instructions and procedures for specific security incident levels. The SOC and the Customer will jointly manage contact procedures.

User Access

The ActiveEye Portal provides the ability to add, update, and remove user access. Every ActiveEye user can save queries, customize reports, and set up daily email summaries. Users may be given administrative access, allowing them to perform administrative tasks, such as setting up new service connectors, resetting passwords, and setting up multi-factor authentication for other users.

1.6.5.1.3 ActiveEye Remote Security Sensor

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

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

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

Specifications	Requirements
Rack Space	1U
Power Consumption (Max)	550 Watts (Redundant Power Supply)
Power Input	100-240V AC
Current	3.7 A – 7.4 A
Circuit Breaker	Qty. 2
Line Cord	NEMA 5-15P
Heat Dissipation (max)	2107 BTU/hr
Internet Service Bandwidth	Bandwidth throughput 10Mbps per zone

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

1.6.5.1.4 Internetworking Firewall

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

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

Specifications	Requirement
Rack Space	1U
Power Consumption (Max)	28.6 W (Single Power Supply)
Power Input	100-240V AC
Current	.52 A
Circuits Breaker	Qty. 1
Heat Dissipation (Max)	97.6 BTU/hr
Line Cord	NEMA 5-15P



Specifications	Requirement
Internet Service Bandwidth	Bandwidth throughput 10 MB High availability Internet Connection (99.99% (4-9s) or higher). Packet loss < 0.5%. Jitter <10 ms. Delay < 120 ms. RJ45 Port Speed - Auto Negotiate

1.6.5.2 Service Modules

ActiveEye delivers service capability by integrating one or more service modules. These modules provide ActiveEye analytics more information to correlate and a clearer vision of events on East Bay Regional Communications System Authority’s network. In addition, modules enable security teams and analysts to more easily access and compare data from these disparate systems. The following subsections describe each ActiveEye service module in detail.

1.6.5.2.1 Log Collection / Analytics

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

Collected events will be stored in the ActiveEye Security Management Platform to enable historical searching or threat hunting as needed. Some high volume, repetitive logs may be aggregated as noted in the documentation. The default storage time period is one year, but no longer than 90 days, following expiration or termination of the Agreement. A longer time period can be provided if subscribed, see Table 1-11: Service Modules for subscription details.

1.6.5.2.2 Network Detection

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

1.6.5.2.3 Vulnerability Detection

Vulnerability Detection is available for Control Room CEN components that can be scanned by the assessment tool integrated with the ActiveEye platform.

Vulnerability scans can be conducted as unauthenticated, authenticated, and/or agent based.



Vulnerability scans will be configured to occur on a recurring schedule that meets the customer's operational profile. Scan results will be available to the customer as they are completed.

1.6.5.3 Security Operations Center Services

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

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

1.7 MPLS MAINTENANCE

The following services are included for maintenance of the EBRCSA MPLS network:

- Remote Technical Support
- Advanced Exchange
- Software Subscription Plan

Motorola will work hand in hand with Nokia to perform the responsibilities assigned to them, respectively, in this SOW for Motorola's end user, EBRCSA. The following equipment is covered under this service agreement:

- Forty-two (42) SAR-8 Routers
- Five (5) SAR-18 Routers

The following is a description of the services included.

Technical Support:

- The Service Level Agreement targets apply to Maintained Products running on hardware and software Releases that are in GA (Generally Available) status and consequently will not apply to either pre-GA or Support Ended hardware/software.
 - "Support Ended" means the product has reached its end of life and is no longer sold by Nokia and customer requests for troubleshooting, advice, information or assistance are no longer performed. The Support Ended status is announced to customers publicly and in advance of the date that it is in effect.
- Updates must occur annually at a minimum. However, notwithstanding the foregoing, an immediate update is required if the Customer increases the quantity of the Maintained Products by more than 10% at any time.
- Prices are based upon purchase of Maintenance Services for the entire agreed Term. Accordingly, and notwithstanding any other provision of the Agreement, Customer may not terminate this SOW, or any order pursuant to this SOW, in whole or in part, for convenience during the Initial Term or any Renewal Term.
- Preventive maintenance of the MPLS equipment is not included.



Repair and Exchange Service - Advanced Exchange Service (RES-AE):

- Repaired or exchanged Parts may contain components that are used, remanufactured or refurbished. Exchanged Parts will be Form, Fit and Functionally compatible.
- RES does not include:
 - Part modification or upgrade.
 - Root cause analysis that specifies the actual Part failure cause or any specific remedial action.
 - Repair or exchange of Parts with defects or malfunctions caused directly or indirectly by: (1) failure of non-Seller personnel to follow the manufacturer's installation, operation, or maintenance instructions; (2) Products or their Parts not specifically identified as RES Entitled Products or RES Entitled Parts; (3) abuse, misuse, or negligent acts of non-Seller personnel; (4) damage from fire, water, wind, exposure to weather, or other forces of nature; (5) acts of terrorism, vandalism or other hostiles actions.
 - Repair or exchange of Parts that show evidence of: (1) improper packaging; (2) improper handling; (3) modification by non-Seller approved personnel; (4) the installation or attachment of non-Seller or non-OEM approved components including hardware or software; (5) any condition that exceeds the tolerances as prescribed by the manufacturer.
 - Passive and mounting hardware such as cabinets, chassis, frames, antennae, connectors, cables, cable assemblies, cords, brackets, bezels, faceplates, adapters, panels or labels.
 - Consumables such as batteries, air filters, or transformers.
 - Documentation or software in all media forms.

Software Subscription Plan (SSP):

- License Terms of Feature Releases: All software that is provided in connection with the Service is licensed subject to the same terms, restrictions, and limitations as contained in the licenses under which the original software was acquired.
- The following items must be purchased separately by Customer:
 - Any modifications to any parts of the network which are deemed by Motorola/Nokia necessary to accomplish network compatibility with a Feature Release.
 - Any additional products required to take advantage of any new functionality within a Feature Release.
 - Any additional software licenses required to support growth in the network of hardware or software (e.g. nodes, DSL ports, subscribers, seats, etc.).
 - Any features in a Feature Release for which an additional license or activation fee is normally required.

Additional Notes:

- If Customer terminates the Agreement prior to the expiration of the Term, termination fees and pending liabilities will need to be settled prior to a future re-subscription to this Service.
- SSP does not include performing the installation of the software releases in Customer's network.
 - Prices are based upon purchase of the Service for the entire agreed Term. Accordingly, and notwithstanding any other provision of the Agreement, there is no right by Customer to terminate this SOW or any order for convenience during the course of the Initial Term or any Renewal Term.

- Where required, a minimum of twelve (12) weeks lead-time must be provided for all Firmware orders (i.e. PROMs – Programmable Read-Only Memory).
- Motorola/Nokia will provide access to Patch Releases or Maintenance Releases for Maintained Products, when available. EBRCSA shall provide its own means to install such fixes, patches, and updates, as and when made available.
- Motorola/Nokia will provide standard instructions for installation of Patch Releases or Maintenance Releases to Customer.
- Feature Releases, Patch Releases and Maintenance Releases will be distributed via Internet download, CD, DVD, tape, or file transfer protocol (FTP).
- EBRCSA agrees to regularly upgrade the network to use the latest available software and firmware releases.
- Motorola/Nokia may deny access immediately and in the future to individuals using the download site other than as permitted.
- If Customer is not forthcoming with updates to the “Products Covered”, Customer shall allow Motorola/Nokia to perform an audit of their network, at EBRCSA’s expense.
- Possible New Release Roadmaps: The forecast of future software releases (product roadmap) is provided by Motorola/Nokia solely to inform EBRCSA of Nokia’s plan of record for the relevant product(s) and both parties to this SOW hereby agree that such information does not form a commitment of any kind on either party in relation to this contract. There are no penalties, liquidated damages or other remedies associated with changes to the product roadmap including cancellation of any specific feature or functionality or delay in the timing of development.
- The maintenance and support commitment is based on support availability for a functionally similar application as furnished by Motorola/Nokia and does not warrant support for specific products, individual features, specific functionalities or legacy interfaces for which there is no broad market demand. In the event that any products or constituent parts in the network are discontinued to the extent that appropriate support cannot be extended, EBRCSA agrees to refresh the complete network, or parts thereof, to Generally Available and fully supported Hardware and Software. Motorola/Nokia shall provide quotes for equipment, software and management system refresh upon request. EBRCSA acknowledges that product/network refresh cycles may necessitate the need for mutually agreed and scheduled network downtime.
- Alternatively, products designated as Future Discontinued, Manufacturer Discontinued or Support Discontinued can be still be supported under the Life Extender Services (degrading SLAs).
- Mature products classified under Extended Life cycle support are subject to reduced target SLAs for non-critical issues.
- On-site support is not specifically provided as part of this SOW. If Motorola/Nokia determines that the issue cannot be restored or resolved remotely, Motorola/Nokia may, at its sole discretion, provide emergency on-site support. In the event on-site intervention is performed, the travel time to arrive at the Site will be added to the Restore time target or discounted from the Restore interval.
- EBRCSA shall at its risk and expense provide Motorola/Nokia with the necessary infrastructure to complete a remote connection to the Site. The preferred tool is RAMSES or any other mutually approved tool.
- A Remote Connection with the following mandatory characteristics must be available:
 - Secure solution based on a permanent LAN to LAN IPSEC using efficient security solution (e.g., firewall)
 - Minimum bandwidth of 2Mbits/s in both directions

- Transfer file system enabling large file transfer through secure connections (e.g., SFTP)
- Multi session system enabling a parallel connection of experts, through secure connections (e.g., SSH)
- The Remote Connection should not:
 - Require a dedicated internet line
 - Rely on any hardware token system
 - If, due to reasons beyond the control of Nokia, the Remote Connection cannot be established or is established with unsatisfactory quality or bandwidth, the KPIs specified in the “Service Level Agreements” shall be extended for the same period during which the Remote Connection could not be established. In this situation, Nokia reserves the right, and upon consent of Customer, to send skilled personnel to the site to resolve the problem. Separate terms and fees apply.

Technical Support SLA/KPI Notes

If on-site intervention is required to resolve a hardware problem (e.g. replacing a faulty Maintained Products), the Restore target is temporarily suspended during that time period. It will restart once the hardware problem is corrected (e.g. a new or repaired Maintained Product is installed in the network).

Target does not apply when Maintained Products are not installed in redundant configurations, if available. In the highly unlikely event that the correction of a software defect is required to provide a Restore, it will be provided if it already exists within a Maintenance Release of the same major load the customer is running. (e.g. customer is running 7.0 Rel 5, and the fix is available in 7.0 Rel 8.). Outside of this, no new development of software code will be performed to provide a Restore.

If a correction of a software defect is required to provide a Resolve, it will be provided if it already exists within a Maintenance Release of the same major load the customer is running. (e.g. customer is running 7.0 Rel 5, and the fix is available in 7.0 Rel 8.). Outside of this, no new development of software code will be performed to provide a Resolve.

Figure 1-3:SLA Targets for Technical Support (TS)

Service Level		Gold		
Welcome Center		24/7		
AR Problem Classification		Critical	Major	Minor
Technical Support	Support Window	24/7		
	Respond	30 M	1 H	NBD
	Restore	6 H	12 H*	
	Resolve	45 CD	90 CD**	NT
KPI Achievement		92%		

Legend:
AR = Assistance Request (trouble ticket)
BD = Business Day of applicable Nokia technical support facility
BH = Business Hours of applicable Nokia technical support facility
CD = Calendar Day
D = Day
H = Hours
M = Minutes
NBD = Next Business Day of applicable Nokia technical support facility
NT = No Target. Nokia will use commercially reasonable efforts to perform the corresponding activity, if feasible at ALU's sole discretion.

MPLS MAINTENANCE TERMS AND CONDITIONS

Definition of Severity Levels

“Critical” (Severity Level 1 or SL1): The system is inoperative and Customer’s inability to use the product has a critical effect on Customer’s operations. This condition is generally characterized by complete system failure and requires immediate correction. In addition, any condition that may critically impact human safety is considered a Severity Level 1 Critical problem.

“Major” (Severity Level 2 or SL2): The system is partially inoperative but still usable by Customer. The inoperative portion of the product severely restricts Customer’s operations, but has a less critical effect than a Severity Level 1 condition.

“Minor” (Severity Level 3 or SL3): The system is usable by Customer, with little or limited impact to the function of the system. This condition is not critical and does not severely restrict overall Customer operations.

Definitions of TS Key Performance Indicators

“Respond Time” (Specialist Call-back): The time period from when Customer first notifies the Motorola/Nokia of a reported problem to when an Nokia expert attempts to contact Customer via telephone or preferred contact method as defined when submitting the request. In the event Motorola/Nokia is unable to contact Customer after three (3) attempts, the ticket will be closed.

“Restore Time” (Remote Neutralization): The time from when Motorola/Nokia is contacted and an event is determined to be loss of service and/or functionality affecting, to the time when Motorola/Nokia provides the means to return a system to operational status.

“Resolve Time” (Final Resolution Time): The time from when Customer first notifies the Motorola/Nokia to the time when a procedural solution/fix to address the issue is made available to Customer. This may occur simultaneously with Restore Time, unless the Restore Time is by means of a temporary workaround and Motorola/Nokia determines that a more suitable permanent solution can feasibly be provided.

Service Level Agreement (SLA) Targets

SLA Targets specify the performance objectives in terms of KPIs by severity level. SLA Targets vary depending on the maintenance coverage selected (see SLA Target table).

Patch Releases/Maintenance Releases

TS Service includes only patch releases and maintenance releases as may be made available for Motorola/Nokia Maintained Products during the Term for use with Maintained Products. TS Service does not include access to feature releases. Decisions of which

versions of software will be updated, and whether to include a correction in a maintenance release as opposed to including it in the next feature release, rests in Motorola/Nokia's sole discretion. TS Service does not entitle or support EBRCSA to use optional or new software features resident in a maintenance release or feature release, except to the extent that EBRCSA has separately paid the applicable license fees for the use thereof. Motorola/Nokia shall have the sole right to determine whether a new functionality shall be included in a feature release or as an optional software feature.

License Terms

All software that is ultimately provided in connection with TS Service including, without limitation, maintenance releases, patch releases or workarounds, are licensed subject to the same terms, restrictions, and limitations as contained in the licenses under which the original software was acquired.

1.8 NICE GOLD LITE MAINTENANCE SERVICES

A renewal of the NICE Gold Lite maintenance services is included. The following table summarizes the system services covered in the NICE Gold Lite package and the priority levels:

Gold Lite Level Coverage Description:				
Service	Gold Lite			
Phone & Remote Support Coverage	24 X 7			
On Site Support- Restrictions Apply	8- 5 M-F			
CSC Access 24 X 7	Yes			
Remote Diagnosis	Yes			
Escalation	Yes			
Repair and Replacement of failed parts	Yes			
Gold Lite	Priority 1	Priority 2	Priority 3	Priority 4
Phone Availability	24*7	24*7	24*7	24*7
Support Coverage	8- 5*5	8 – 5*5	8- 5*5	8- 5*5
Call Back Response Time	60 minutes	120 minutes	24 hours	24 hours
On Site Response Times	6 hours	24 hours	48 hours	48 hours
Priority 1	An incident that results in a critical impact on hardware, software or communications to the NICE Production System, where customer experiences a complete or imminent loss of recording or data and there is no workaround solution.			
Critical				
Priority 2	A major problem that results in loss of ability to retrieve calls or loss of replay functionality for two or more workstations.			
High				
Priority 3	A product anomaly that affects one or more workstations, but does not result in a loss of recording or replay. Product response or performance is diminished intermittently, or issues impacting several users occur, such as loss of system administrator's ability to add or delete users.			
Medium				
Priority 4	An incident that has no business impact on a Production System, such as system inquiry, planned intervention requests for documentation, or request for information.			
Low				

1.8.1 NICE SUA

The intent of the SUA is to keep the Customer system on supportable versions for the term of the contract. Upgrades to NICE products will be delivered in conjunction with a Motorola

ASTRO System upgrade. Any requests for upgrades outside of an ASTRO System upgrade project may be subject to additional fees. EBRCSA is eligible for up to five software upgrades and up to one hardware upgrade throughout the six years of support.

Upgrades will be limited to 'like-for-like' updates. Upgrades will be limited to the products and features that were originally included in the contract. Upgrades under an SUA contract will not include new features, new applications, or system expansions. Content of an upgrade (software and hardware) is within the sole discretion of NICE.



SECTION 2

ASTRO SYSTEM UPGRADE AGREEMENT (SUA II) STATEMENT OF WORK

2.1 OVERVIEW

Utilizing the ASTRO System Upgrade Agreement II (“SUA II”) service, the ASTRO system is able to take advantage of new functionality and security features while extending the operational life of the system. Motorola Solutions continues to make advancements in on premise 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. In addition, the SUA II may provide specified ASTRO platform migrations if and when necessary based on ASTRO software support.

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

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

2.2 SCOPE

As system releases become available, Motorola Solutions will provide the Customer with the software, hardware and implementation services required to execute up to one system infrastructure upgrade in each eligible upgrade window over the term of the agreement. The term of the agreement is listed in Table 2-1: SUA II Term. Motorola Solutions will deliver up to one upgrade within each period. The eligible upgrade windows and their duration are illustrated in Table 2-2: Eligible Upgrade Window.

With the addition of the cloud services, Motorola Solutions 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 release upgrades and will occur outside the defined eligible upgrade windows in Table 2-2: Eligible Upgrade Window. Motorola Solutions may in its sole discretion automatically apply the cloud updates as they become available.

If needed to perform the software upgrades, Motorola Solutions will provide updated and/or replacement hardware for covered infrastructure components. System release upgrades, when executed, will provide an equivalent level of functionality as that originally purchased and deployed by the Customer. At Motorola Solutions’ option, new system releases may introduce new features or enhancements that Motorola Solutions may offer for purchase. These new features, available separately for purchase, are not part of the SUA II.



Table 2-1: SUA II Term

Duration	6 Year(s)
-----------------	-----------

Table 2-2: Eligible Upgrade Window

First Eligible Upgrade Window	Second Eligible Upgrade Window	Third Eligible Upgrade Window
Duration:	Duration:	Duration:
2024 - 2025	2026 - 2027	2027 - 2028

The methodology for executing each system upgrade is described in Section 2.5.3: System Upgrades. ASTRO SUA II pricing is based on the system configuration outlined in Section 4.1 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 II price adjustment.

The price quoted for ASTRO SUA II requires the Customer to choose a certified system upgrade path in Section 2.7: ASTRO System Release Upgrade Paths. Should the Customer elect an upgrade path other than one listed in Section 2.7: ASTRO System Release Upgrade Paths, the Customer agrees that additional fees may be incurred to complete the implementation of the system upgrade. In this case, Motorola Solutions will provide a price quotation for any additional materials and services necessary.

2.3 INCLUSIONS

The ASTRO SUA II only covers the products outlined in Section 4.1 System Pricing Configuration and does not cover all products. Refer to Section 2.4: Limitations and Exclusions for examples of exclusions and limitations.

The ASTRO SUA II applies only to system release 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.

ASTRO SUA II makes available the subscriber radio software releases that are shipping from the factory during the coverage period.

2.4 LIMITATIONS AND EXCLUSIONS

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

Excluded Products and Services	Examples but not limited to
Purchased directly from a third party	NICE, Genesis, Verint
Residing outside of the ASTRO network	CAD, E911, Avtec Consoles
Not certified on ASTRO systems	Laptops, PCs, Eventide loggers
Backhaul Network	MPLS, Microwave, Multiplexers
Two-Way Subscriber Radios	APX, MCD 5000, Programming, Installation

Excluded Products and Services	Examples but not limited to
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

2.4.1 Non-Standard Configurations

Systems that have non-standard configurations that have not been certified by Motorola Solutions Systems Integration Testing are specifically excluded from the ASTRO SUA II 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.

2.4.2 System Expansions and New Features

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

Any implementation services that are not directly required to support the certified system upgrade and/or platform migration are not included. Unless otherwise stated, implementation services necessary to provide system expansions and/or new features or functionality that are implemented concurrently with the certified system upgrade are not included.

2.4.3 Security Update Service

ASTRO SUA II does not cover or include deliverables included with the Security Update Service. The SUA II does not include software support for virus attacks, applications that are not part of the ASTRO system, unauthorized modifications or other misuse of the covered software. At the time of upgrade, Motorola Solutions will provide the latest applicable software, patches and antivirus updates when and if available, as a part of the system release upgrade. The security patches and antivirus updates delivered as part of this upgrade are intended to bring the system current in all respects but does not imply that the Customer is eligible for ongoing security patching.

ASTRO SUA II does not cover the labor or materials associated with the backlog accumulation of security patches or antivirus updates. Additional fees may apply as outlined in Section 2.5.1.1: Motorola Solutions Responsibilities.

The upgrade may include 3rd party software such as Microsoft Windows and Server OS, Red Hat Linux, and any Motorola Solutions software service packs that may be available. Motorola Solutions will only provide patch releases that have been analyzed, pre-tested, and certified in a dedicated ASTRO test lab to ensure that they are compatible and do not interfere with the ASTRO network functionality.



2.5 SYSTEM UPGRADES

2.5.1 Upgrade Planning and Preparation

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

2.5.1.1 Motorola Solutions 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 project schedule identifying key tasks and personnel resources required from Motorola Solutions and Customer for each task and phase of the 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 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 Solutions will provide this training only once per system.

2.5.1.2 Customer Responsibilities

- Contact Motorola Solutions to schedule and engage the appropriate Motorola Solutions resources for a system release upgrade and provide necessary information requested by Motorola Solutions to execute the upgrade. Review upgrade schedule and reach mutual agreement of the same.
- Identify hardware not purchased through Motorola Solutions that will require the system release upgrade software.
- Purchase the security patches, antivirus upgrades and the labor necessary to address any security upgrades backlog accumulation identified in Section 1.5.1: Motorola Solutions 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 Solutions 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 Solutions will provide the network connection specifications, as listed in Section 1.5.1: Motorola Solutions Responsibilities. Network connectivity must be provided at least 12 weeks prior to the scheduled upgrade. In the event access to a network connection is unavailable, the Customer may be billed additional costs to execute the system release 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 release upgrade when applicable. Upon reasonable request by Motorola Solutions, 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 4.1 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 Solutions under separate Agreement.
- Participate in release impact training at least 12 weeks prior to the scheduled upgrade. This applies only to primary zone core owners. It is the zone core owner's responsibility to contact and include any user agencies that need to be trained, or to act as a training agency for those users not included.

2.5.2 System Readiness Checkpoint

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

2.5.2.1 Motorola Solutions 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 Solutions 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.

2.5.2.2 Customer Responsibilities

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



2.5.3 System Upgrade

2.5.3.1 Motorola Solutions Responsibilities

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

2.5.3.2 Customer Responsibilities

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

2.5.4 Upgrade Completion

2.5.4.1 Motorola Solutions Responsibilities

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

2.5.4.2 Customer Responsibilities

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

2.6 SPECIAL PROVISIONS

The migration of capabilities from ASTRO on premise 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 Solutions roadmap and may be subject to additional cloud terms and conditions.

The SUA does not extend to customer-provided software and hardware. Motorola Solutions 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 Solutions 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 Solutions system release. This includes, but is not limited to, Motorola Solutions costs for the deployment of resources to implement the upgrade once the limitations have been resolved by the customer.

Any Motorola Solutions software, including any system releases, is licensed to Customer solely in accordance with the applicable Motorola Solutions Software License Agreement. Any non-Motorola Solutions 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 Solutions the right to sublicense the Non-Motorola Solutions 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 Solutions makes no representations or warranties of any kind



regarding non-Motorola Solutions Software. Non-Motorola Solutions Software may include Open Source Software.

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

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

The ASTRO SUA II annualized price is based on the fulfillment of the system release upgrade in each eligible upgrade window. If the Customer terminates, except if Motorola Solutions 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 and the balance of payments owed in the SUA II contract term if any platform migration has been completed prior to the point of termination.

The customer is covered for the specified platform migrations listed in Section 2.3: Inclusions. Specified platform migrations may be performed in conjunction with or separately from the eligible system upgrades. MSI will work with the customer during the upgrade planning process to determine the best methodology and timing based on the level of effort and the customer's operational needs.

2.7 ASTRO SYSTEM RELEASE UPGRADE PATHS

The upgrade paths for standard ASTRO system releases are listed in Table 2-3: Certified Standard ASTRO System Release Upgrade Paths.

Table 2-3: Certified Standard ASTRO 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 2-4: Certified High Security ASTRO System Release Upgrade Paths.

Table 2-4: Certified High Security ASTRO 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 7.x platform is expressed in the form “ASTRO 7.x release 20YY.Z”. In this taxonomy, YY represents the year of the release, and Z represents the release count for that release year.

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

- 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 Solutions’ 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 Solutions reserves the right to make changes to the content and timing of any product, product feature, or software release.



SECTION 3

MANAGED DETECTION AND RESPONSE STATEMENT OF WORK

3.1 OVERVIEW

In accordance with the terms and conditions of the Agreement, this Statement of Work (SOW), including all of its subsections and attachments, defines the principal activities and responsibilities of all parties for the delivery of Motorola Solutions, Inc. (Motorola Solutions) Cybersecurity services as presented in this proposal to East Bay Regional Communications System Authority (hereinafter referred to as “Customer”).

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

3.2 DESCRIPTION OF SERVICE

3.2.1 Deployment Timeline and Milestones

To initiate the ASTRO 25 Managed Detection and Response service to function, Motorola Solutions and the Customer must perform deployment tasks. Service deployment is broken into the following phases, each with specific deliverables.

Phase 1: Information Exchange

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

Phase 2: Infrastructure Readiness

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

Phase 3: System Buildout and Deployment

Motorola Solutions will build and provision tools in accordance with the requirements of this proposal and consistent with information gathered in earlier phases. Motorola Solutions will also provide detailed requirements regarding Customer deployment actions. The Customer must deploy tools, as applicable, in their environment, in accordance with provided requirements.



Phase 4: Monitoring Turn Up

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

Phase 5: Tuning and Customer Training

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

3.2.2 General Responsibilities

3.2.2.1 Motorola Solutions Responsibilities

- Provide, maintain, and when necessary, repair under warranty hardware and software required to monitor the ASTRO 25 network and applicable CEN systems Inclusive of the AERSS and all software operating on it.
 - If the Centralized Event Logging feature is not installed on the Customer's ASTRO 25 RNI, Motorola Solutions will install it as part of this service.
- Coordinate with the Customer on any system changes necessary to integrate the AERSS into the system and establish necessary connectivity.
- Provide software and licenses to the Customer necessary to remotely monitor the ASTRO 25 network and applicable CEN environments.
- Verify connectivity and monitoring is active prior to start of service.
- Coordinate with the Customer to maintain Motorola Solutions service authentication credentials.
- Maintain trained and accredited technicians.
- Monitor the Customer's ASTRO 25 network and applicable CEN systems 24/7/365 for malicious or unusual activity.
- Respond to security incidents in the Customer's system in accordance with Section 3.3.6: Priority Level Definitions and Notification Times. This may include, but is not limited to, requesting additional information from the Customer, continuing to monitor the event for further development or informing the Customer to enact the Customer's documented Incident Response plan.
- Ensure that all monitored devices within the network are properly configured for Syslog, forwarding events to the centralized event log server.
- 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 Security Management platform, so the Customer can access security event and incident details.

3.2.2.2 Customer Responsibilities

- The ASTRO 25 Managed Detection and Response service requires a connection from the Customer's ASTRO 25 network and applicable CEN systems to the Internet. Establish connectivity with sufficient bandwidth before service commences. Internet service bandwidth requirements are as follows:



- Bandwidth throughput of 10Mbps per zone.
- 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
- Maintain an active Security Update Service (SUS) subscription, ensuring patches and antivirus definitions are applied according to the release cadence of the service.
- If a Control Room CEN is included, it will require a static gateway IP and sufficient capacity on the switch (3 ports – 2 active connections and 1 mirror port).
- Allow Motorola Solutions continuous remote access to monitor the ASTRO 25 network and applicable CEN systems. This includes keeping the connection active, providing passwords, and working with Motorola Solutions to understand and maintain proper administration privileges.
- Provide continuous utility service(s) to any Motorola Solutions equipment installed or utilized at the Customer's premises to support service delivery.
- Provide Motorola Solutions with contact information necessary to complete the Customer Support Plan (CSP). Notify the assigned Customer Support Manager (CSM) in advance of any contact information changes.
- Notify Motorola Solutions if any new components are added to or removed from the environment as it may be necessary to update or incorporate in Managed Detection and Response. Changes to monitored components may result in changes to the pricing of the Managed Detection and Response service.
- As necessary, upgrade the ASTRO 25 system, on-site systems, and third party software or tools to supported releases.
- Allow Motorola Solutions' dispatched field service technicians physical access to monitoring hardware when required.
- Cooperate with Motorola Solutions and perform all acts that are required to enable Motorola Solutions to provide the services described in this SOW.
- Configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a port(s) on a switch) network traffic to the ActiveEye sensor for applicable CEN systems.
- Responding to Cybersecurity Incident Cases created by the Motorola Solutions Security Operations Center.

3.2.3 Service Modules

The following subsections describe the delivery of the service modules selected in Table 1-11: Service Modules.

3.2.3.1 Log Analytics

Motorola Solutions Responsibilities

- Consult with and advise the Customer on performing necessary system configurations to direct log sources to the appropriate Remote Security Sensor.

- Configure Customer's networking infrastructure to allow AERSS to Communicate with ActiveEye as defined.
- The SOC will consult with the Customer to identify appropriate log sources for the level of threat detection desired in each environment.

Customer Responsibilities

- 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.

3.2.3.2 Network Detection

Motorola Solutions Responsibilities

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

Customer Responsibilities

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

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

3.2.3.3 Vulnerability Detection

Motorola Solutions Responsibilities

- Configure scans to match the Customer's preferences for depth, scope, and schedule.
- Verify that vulnerability scans are operating properly on the determined schedule.
- Support the Customer in troubleshooting scheduled scan issues.
- The SOC consults with the Customer on a desired attach surface management plan and then configures scan depth, scope, and schedule. The SOC will monitor and verify the scans at a determined schedule.

Customer Responsibilities

- Configure networking infrastructure to allow vulnerability sensors to communicate with centralized server components.
- Perform any remediation actions required to address identified vulnerabilities.
- In the case of authenticated scans, the Customer is responsible for maintaining up to date credentials in the vulnerability scanning platform.



- Work with Motorola Solutions to configure scans to match the Customer's preferences for depth, scope, and schedule.
- Perform any remediation actions required to address identified vulnerabilities.

Applies to the Control Room CEN only.

3.3 SECURITY OPERATIONS CENTER MONITORING AND SUPPORT

3.3.1 Scope

Motorola Solutions will start monitoring the ASTRO 25 Managed Detection and Response service in accordance with Motorola Solutions processes and procedures after deployment, as described in Section 3.2.1: Deployment Timeline and Milestones.

The SOC receives system-generated alerts 24x7, and provides the Customer with a toll-free telephone number and email address for support requests, available 24x7. Support requests are stored in a ticketing system for accountability and reporting. The SOC will respond to detected events in accordance with Section 3.3.6: Priority Level Definitions and Notification Times.

3.3.2 Ongoing Security Operations Center Service Responsibilities

Motorola Solutions Responsibilities

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

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

Customer Responsibilities

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



3.3.3 Technical Support

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

Motorola Solutions Responsibilities

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

Customer Responsibilities

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

Limitations and Exclusions

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

3.3.4 Incident Response

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

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

Motorola Solutions Responsibilities

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

Customer Responsibilities

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



3.3.5 Event Response and Notification

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

Table 3-1: Event Handling

Event Type	Details	Notification Requirement
False Positive or Benign	Any event(s) determined by Motorola Solutions to not likely have a negative security impact on the organization.	None
Event of Interest (EOI)	Any event(s) determined by Motorola Solutions to likely have a negative security impact on the organization.	Escalate to Customer in accordance with routine notification procedure. Escalate in accordance with urgent notification procedure when required by agreed-upon thresholds and SOC analysis. Notification procedures are included in Table 3-2: Notification Procedures.

Notification

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

Table 3-2: Notification Procedures

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

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

Tuning

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

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



Tuning Period Exception

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

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

3.3.6 Priority Level Definitions and Notification Times

Motorola Solutions will analyze events created and/or aggregated by the ASTRO® 25 Managed Detection and Response services, assess their type, and notify the Customer in accordance with the following table.

Table 3-3: Priority Level Definitions and Notification Times

Incident Priority	Incident Definition	Notification Time
Critical P1	<p>Security incidents that have caused, or are suspected to have caused significant and/or widespread damage to the functionality of Customer’s ASTRO 25 system or information stored within it. Effort to recover from the incident may be significant.</p> <p>Examples:</p> <ul style="list-style-type: none"> • Malware that is not quarantined by anti-virus. • Evidence that a monitored component has communicated with suspected malicious actors. 	<p>Response provided 24 hours, 7 days a week, including US Holidays.</p>
High P2	<p>Security incidents that have localized impact, but are viewed as having the potential to become more serious if not quickly addressed. Effort to recover from the incident may be moderate to significant.</p> <p>Examples:</p> <ul style="list-style-type: none"> • Malware that is quarantined by antivirus. • Multiple behaviors observed in the system that are consistent with known attacker techniques. 	<p>Response provided 24 hours, 7 days a week, including US Holidays.</p>
Medium P3	<p>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.</p> <p>Examples:</p> <ul style="list-style-type: none"> • 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. 	<p>Response provided Monday through Friday 8 a.m. to 5 p.m. local time, excluding US Holidays.</p>

Incident Priority	Incident Definition	Notification Time
Low P4	These are typically service requests from Customer.	Response provided Monday through Friday 8 a.m. to 5 p.m. local time, excluding US Holidays.



3.4 LIMITATIONS AND EXCLUSIONS

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

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

3.4.1 Service Limitations

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

3.4.2 Processing of Customer Data in the United States and/or other Locations

Customer understands and agrees that data obtained, accessed, or utilized in the performance of the services may be transmitted to, accessed, monitored, and/or otherwise processed by Motorola Solutions in the United States (US) and/or other Motorola Solutions 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.

3.4.3 Customer and Third-Party Information

Customer understands and agrees that Motorola Solutions may obtain, use and/or create and use anonymized, aggregated and/or generalized Customer data, such as data relating to actual and potential security threats and vulnerabilities, for its lawful business purposes, including improving its services and sharing and leveraging such information for the benefit of Customer, other customers, and other interested parties. For purposes of this engagement, so long as not specifically identifying the Customer, Customer data shall not include, and Motorola Solutions shall be free to use, share and leverage security threat intelligence and mitigation data generally, including without limitation, third party threat vectors and IP addresses, 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.



3.4.4 Third-Party Software and Service Providers, including Resale

Motorola Solutions 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, EULAs, privacy statements, data processing agreements and/or other applicable terms. Such third-party providers and terms are available publicly, through performance, or upon request.

Motorola Solutions disclaims any and all responsibility for any and all loss or costs of any kind associated with security events. Motorola Solutions 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.



SECTION 4

PRICING SUMMARY

4.1 SYSTEM PRICING CONFIGURATION

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

Table 4-1: System Configuration

System Configuration	
Master Site Configuration	
On-Premise Master Site	1
System Level Features	
ISSI 8000	2
Network Management Clients	3
Unified Network Services (UNS) or KMF	1
Security Configuration	
CEN	1
Firewalls	4
RF Site Configuration	
IP Simulcast Prime Sites	6
RF Sites (include Simulcast sub-sites, ASR sites, HPD sites)	35
GTR 8000 Base Stations	421
Dispatch Site Configuration	
Dispatch Site Locations	33
MCC7500 Dispatch Consoles	223
AIS	8
CCGWs	114
Aux I/O	40
Third Party Elements	
NICE:	
Single NIR Recorder Base Bundle	3
NIR Logging Backup/Replacement Server	3
APCO P25 TR Channel Premium	360
DL380 Applications Server	4
Inform Professional channel license	360
Evidence Compliance PACK (Organizer and Media Player)	360
HP 6TB 6G SAS HDD for Gen10 ML350 or DL380	8
17" LCD Drawer, Keyboard, Mouse, KVM 8 ports, Cables - Supports IP Connections	1

4.2 INFRASTRUCTURE SUA AND MAINTENANCE PRICING

Motorola is pleased to provide the following services to East Bay Regional Communications System Authority. This pricing is based on services proposed for the term shown below. Any changes to the services proposed or the term will require a change order.

	2023/24	2024/25	2025/26	2026/27	2027/28	2028/29	TOTAL
ASTRO Maintenance	\$1,478,718	\$1,537,867	\$1,599,381	\$1,663,410	\$1,729,952	\$1,799,156	\$9,808,484
ASTRO SUA	\$1,368,746	\$1,401,210	\$1,434,973	\$1,470,086	\$1,506,604	\$1,544,583	\$8,726,201
MPLS	\$96,455	\$100,313	\$104,325	\$108,498	\$112,838	\$129,416	\$651,846
MDR	\$290,154	\$301,760	\$313,830	\$326,384	\$339,439	\$353,016	\$1,924,583
NICE SUA and Maintenance	\$322,951	\$286,144	\$306,213	\$327,802	\$351,032	\$376,039	\$1,970,180
TOTAL	\$3,557,023	\$3,627,293	\$3,758,723	\$3,896,180	\$4,039,866	\$4,202,211	\$23,081,295

4.3 MAINTENANCE AND SUA PAYMENT TERMS

Motorola will invoice Customer annually in advance of each year of the plan.

4.4 MANAGED DETECTION AND RESPONSE PAYMENT SCHEDULE & TERMS

Period of Performance

The initial subscription period of the contract will extend six (6) years from the Commencement Date of Service, defined as the date data is available for analysis, or not later than thirty (30) days after Motorola provides the Customer with necessary hardware or software to connect the first data source.

Term

The Term of the contract begins on the Commencement Date of Service and remains in effect until the expiration of the initial period so specified.

Billing

Upon acceptance of this proposal by the Customer, Motorola Solutions customer affirms that a purchase order or notice to proceed is not required for contract performance or for subsequent years of service and Motorola Solutions will invoice the Customer for all service fees in advance for the full Year 1 amount according to the Pricing table in Section **Error! Reference source not found..3**.

Thereafter, Motorola Solutions will invoice the Customer annually, in advance for (a) the Services to be performed (as applicable); and (b) any other charges incurred as agreed upon between the parties during the term of the subscription.



Customer will make payments to Motorola within thirty (30) days after receipt of each invoice. Customer will make payments when due in the form of a check, cashier's check, or wire transfer drawn on a United States financial institution.

INFLATION ADJUSTMENT. 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. Measurement will take place once the annual average for the new year has been posted by the Bureau of Labor Statistics. 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).

Tax

Unless otherwise noted, this proposal excludes sales tax or other applicable taxes (such as Goods and Services Tax, Value Added Tax and other taxes of a similar nature). Any tax the customer is subject to will be added to invoices.



SECTION 5

CONTRACTUAL DOCUMENTATION

AMENDMENT NO. 5

TO COMMUNICATIONS SYSTEM AGREEMENT

This Amendment No. 5 to the Communications System Agreement (this "Amendment No. 5") is entered into and effective as of the date of the last signature hereto ("**Amendment Effective Date**") by and between **East Bay Regional Communications System Authority** (the "Customer") and **Motorola Solutions, Inc.**, formerly Motorola, Inc. ("Motorola") each of which may alternatively be referred to herein as a "**Party**" and collectively as the "**Parties**".

RECITALS

WHEREAS, Customer and Motorola previously entered into a Communications System Agreement fully executed on July 7, 2009 (the "CSA").

WHEREAS, Customer and Motorola previously entered into Amendment No. 1 to the CSA, effective July 6, 2012, whereby Sections 3.3 and 3.4 of the original CSA were extended through July 6, 2017. Section 3.4 of the CSA permits the Customer to make additional purchases of Equipment, Software, and services off of the CSA for a stated time period from the Effective Date.

WHEREAS, Customer and Motorola previously entered into an Amendment to the CSA for System Upgrade (SUA) Transactions effective June 28, 2013 (the "SUA Amendment"), whereby the Parties agreed add Motorola's SUA Terms and Conditions to the CSA and add the SUA program to the CSA scope of work to begin in 2013 and continue until June 30, 2023.

WHEREAS, Customer and Motorola previously entered into Amendment No. 2 to the CSA, effective July 6, 2017, whereby Sections 3.3 and 3.4 of the original CSA were extended through July 6, 2020.

WHEREAS, Customer and Motorola previously entered into Amendment No. 3 to the CSA, effective February 9, 2018, to allow other agencies which are Members of Customer to purchase off of the CSA.

WHEREAS, Customer and Motorola previously entered into Amendment No. 4 to the CSA, effective June 19, 2020, to extend the right of the Customer under Section 3.4 of the CSA for an additional three (3) years through July 6, 2023, and to extend the term of the contract under Section 3.3 of the CSA to coincide with this time period or until expiration of any unexpired Warranty Period, whichever occurs last.

WHEREAS, the Parties desire to further amend the CSA as set forth below.



AGREEMENT

NOW THEREFORE, in consideration of the above premises, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereto agree to amend the CSA as follows:

1. The first sentence of Section 3.4 of the CSA is hereby deleted and replaced with:

"Through and including July 6, 2029, the Customer may order additional Equipment or Software, provided it is then available, and related services."

The remainder of Section 3.4 of the CSA is unchanged.
2. Section 3.3 of the CSA is hereby deleted and replaced in its entirety with:

"TERM. Unless otherwise terminated in accordance with the provisions of this Agreement or extended by mutual agreement of the parties, the term of this Agreement shall begin on the Effective Date and shall continue until July 6, 2029."
3. Pursuant to Section 3.1 of the CSA, as amended, attached hereto as Exhibit "A" and incorporated by reference, is added to the Scope of Work, and the Contract Price in Section 5.1 of the CSA is increased by an amount of \$_____.
4. The SUA Terms and Conditions in Section 5 of the SUA Amendment is hereby deleted and replaced in its entirety with Motorola's Maintenance, Support and Lifecycle Management Addendum attached hereto as Exhibit "B" and incorporated by reference.
5. The Cyber Addendum, attached hereto as Exhibit "C" and incorporated by reference, is hereby added to the CSA as a new Addendum 1.
6. The Data Processing Addendum, Attached hereto as Exhibit "D" and incorporated by reference, is hereby added to the CSA as a new Addendum 2.
7. In the event of a conflict between the terms of this Amendment No. 5 and the terms of the CSA, this Amendment No. 5 shall control. All other terms of the CSA, as amended, shall remain unchanged and in full force and effect.

Motorola Solutions, Inc.

By: _____
Name: _____
Title: _____
Date: _____



East Bay Regional Communications System Authority

By: _____

Name: _____

Title: _____

Date: _____



EXHIBIT "A"

EAST BAY REGIONAL COMMUNICATIONS SYSTEM AUTHORITY (EBRCSA) INFRASTRUCTURE SUA AND MAINTENANCE PROPOSAL DATED JUNE 28, 2023

EXHIBIT "B"

MAINTENANCE, SUPPORT AND LIFECYCLE MANAGEMENT ADDENDUM

This Addendum to the Communications System Agreement or other previously executed Agreement currently in force, as applicable ("Primary Agreement") provides additional or different terms and conditions to govern the sale of Maintenance, Support and Lifecycle Management services. The terms in this Addendum are integral to and incorporated into the Primary Agreement signed by the Parties.

1. DEFINITIONS

All capitalized terms not otherwise defined herein shall have the same meaning as defined in the Primary Agreement.

"MUA" means Microwave Upgrade Agreement (MUA).

"NUA" means Network Upgrade Agreement (NUA).

"SUA" or "SUA II" means Motorola's Software Upgrade Agreement program for Motorola's P25 radio system.

2. SCOPE

Motorola will provide Maintenance and Support Services and/or Lifecycle Management as further described in the applicable Statement of Work, or attachment to Motorola's proposal for additional services.

3. TERMS AND CONDITIONS

The terms of the Primary Agreement combined with the terms of this Addendum will govern the products and services offered pursuant to this Addendum. To the extent there is a conflict between the terms and conditions of the Primary Agreement and the terms and conditions of this Addendum, this Addendum takes precedence.

3.1 MAINTENANCE AND SUPPORT SERVICES

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

3.1.2 START DATE. The "Start Date" for Maintenance and Support Services will be indicated in the proposal or a cover page entitled "Service Agreement".

3.1.3 AUTO RENEWAL. Unless the cover page or SOW specifically states a termination date or one Party notifies the other in writing of its intention to discontinue the Services, this Agreement will renew for an additional one (1) year term on every



anniversary of the Start Date. At the anniversary date, Motorola may adjust the price of the Services to reflect the renewal rate.

3.1.4 TERMINATION. Written notice of intent to terminate must be provided thirty (30) days or more prior to the anniversary date. If Motorola provides Services after the termination or expiration of this Addendum, the terms and conditions in effect at the time of termination or expiration will apply to those Services and Customer agrees to pay for those services on a time and materials basis at Motorola's then effective hourly rates.

3.1.5 EQUIPMENT DEFINITION. For maintenance and support services, Equipment will be defined to mean the hardware specified in the applicable SOW or attachments to the maintenance and support proposal.

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

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

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

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

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

3.1.11 EXCLUDED SERVICES.

- a) Service excludes the repair or replacement of Equipment that has become defective or damaged from use in other than the normal, customary, intended, and authorized manner; use not in compliance with applicable industry standards; excessive wear and tear; or accident, liquids, power surges, neglect, acts of God or other force majeure events.
- b) Unless specifically included in this Addendum, Service excludes items that are consumed in the normal operation of the Equipment, such as batteries or magnetic tapes.; upgrading or reprogramming Equipment; accessories, belt clips, battery chargers, custom or special products, modified units, or software; and repair or maintenance of any transmission line, antenna, microwave equipment, tower or tower



lighting, duplexer, combiner, or multicoupler. Motorola has no obligations for any transmission medium, such as telephone lines, computer networks, the internet or the worldwide web, or for Equipment malfunction caused by the transmission medium.

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

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

3.2 LIFECYCLE MANAGEMENT SERVICES

3.2.1 The Software License Agreement included as Exhibit A to the Primary Agreement applies to any Motorola Software provided as part of the Lifecycle Management transactions.

3.2.2 The term of this Addendum is 6 years, commencing on July 1, 2023. The Lifecycle Management Price for the 6 years of services is \$_____, excluding applicable sales or use taxes but including discounts as more fully set forth in the pricing pages. Because the Lifecycle Management is a subscription service as more fully described in the applicable Lifecycle Management Statement of Work, payment from Customer is due in advance and will not be in accordance with any Payment Milestone Schedule.

3.2.3 The System upgrade will be scheduled during the subscription period and will be performed when Motorola's system upgrade operation resources are available. Because there might be a significant time frame between when this Addendum is executed and when a System upgrade transaction is performed, Motorola may substitute any of the promised Equipment or Software so long as the substitute is equivalent or superior to the initially promised Equipment or Software.

3.2.4 Acceptance of a Lifecycle Management transaction occurs when the Equipment (if any) and Software are delivered and the Lifecycle Management services are fully performed; there is no Acceptance Testing with a Lifecycle Management transaction.

3.2.5 The Warranty Period for any Equipment or Motorola Software provided under a Lifecycle Management transaction will commence upon shipment and not on System Acceptance or Beneficial Use, and is for a period of ninety (90) days rather than one (1) year. The ninety (90) day warranty for Lifecycle Management services is set forth in the Lifecycle Management Statement of Work.



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

- a) Upon reasonable request by Motorola, Customer will provide a complete serial and model number list of the Equipment.
- b) Lifecycle Management services exclude the repair or replacement of Equipment that has become defective or damaged from use in other than the normal, customary, intended, and authorized manner; use not in compliance with applicable industry standards; excessive wear and tear; or accident, liquids, power surges, neglect, acts of God or other force majeure events.
- c) Unless specifically included in this Addendum or the Lifecycle Management Statement of Work, Lifecycle Management services exclude items that are consumed in the normal operation of the Equipment; accessories; and repair or maintenance of any transmission line, antenna, microwave equipment, tower or tower lighting, duplexer, combiner, or multicoupler. Motorola has no obligations for any transmission medium, such as telephone lines, computer networks, the internet or the worldwide web, or for Equipment malfunction caused by the transmission medium.
- d) Customer will provide Motorola with designated points of contact (list of names and phone numbers) that will be available during the performance of the Lifecycle Management services.

3.2.7 The Lifecycle Management annualized price is based on the fulfillment of the two year cycle. If Customer terminates this service during a two year cycle, except for Motorola's default, then Customer will be required to pay for the balance of payments owed for the two year cycle if a major system release has been implemented before the point of termination.

3.2.8 If Customer terminates this service and contractual commitment before the end of the 6 year term, for any reason other than Motorola's default, then the Customer will pay to Motorola a termination fee equal to the discount applied to the last three years of service payments related to the 6 year commitment.

4. PAYMENT

4.1 Unless alternative payment terms are stated in this Agreement, Motorola will invoice Customer in advance for each payment period. All other charges will be billed monthly, and the Customer must pay each invoice in U.S. dollars within thirty (30) days of the invoice date. Customer will reimburse Motorola for all property taxes, sales and use taxes, excise taxes, and other taxes or assessments that are levied as a result of Services rendered under this Agreement (except income, profit, and franchise taxes of Motorola) by any governmental entity.

4.2 INFLATION ADJUSTMENT. For multi-year agreements, at the end of the 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 service and subscription 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.

5. ENTIRE AGREEMENT. This Addendum, any related attachments, and the Primary Agreement, constitutes the entire agreement of the Parties regarding the subject matter of this Addendum and supersedes all previous agreements, proposals, and understandings, whether written or oral, relating to this subject matter. This Addendum 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 or purchase order, acknowledgment or other form will not be considered an amendment or modification of this Addendum, even if a representative of each Party signs that document.

END



EXHIBIT "C"

CYBER ADDENDUM

Motorola Solutions Inc. (Motorola Solutions) and the customer named in this Agreement ("Customer") hereby agree as follows:

Section 1. APPLICABILITY

1.1 This Addendum sets out additional and superseding terms applicable to Customer's purchase of cyber security services, including (i) Remote Security Update Service, Security Update Service, and Managed Detection & Response subscription services, among other subscription services, (ii) professional services, and/or (iii) retainer services (i.e., professional services when expressly purchased as a block of pre-paid hours for use, subject to expiration, within a specified period across certain offered service categories (Retainer Services) (all collectively herein, "Services").

Section 2. ADDITIONAL DEFINITIONS AND INTERPRETATION

2.1. **"Customer Contact Data"** means data Motorola Solutions collects from Customer, its Authorized Users, and their end users for business contact purposes, including marketing, advertising, licensing and sales purposes.

2.2 **"Customer Data"** means Customer data, information, and content, provided by, through, or on behalf of Customer, its Authorized Users, and their end users through the use of the Services. Customer Data does not include Customer Contact Data, Service Use Data, or information from publicly available sources or other Third-Party Data or Motorola Solutions Data or anonymized or generalized data. For avoidance of doubt, so long as not specifically identifying the Customer, Customer Data shall not include, and Motorola Solutions shall be free to use, share and leverage security threat intelligence and mitigation data generally, including without limitation, third-party threat vectors and IP addresses, 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.

2.3 **"Feedback"** means comments or information, in oral or written form, given to Motorola Solutions by Customer or Authorized Users, including their end users, in connection with or relating to the Services. Any Feedback provided by Customer is entirely voluntary. Motorola Solutions may use, reproduce, license, and otherwise distribute and exploit the Feedback without any obligation or payment to Customer or Authorized Users. Customer represents and warrants that it has obtained all necessary rights and consents to grant Motorola Solutions the foregoing rights.

2.4 **"Motorola Solutions Data"** means data owned or licensed by Motorola Solutions.

2.5 **"Process"** or **"Processing"** means any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, copying, analyzing, caching, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.



2.6 **“Service Use Data”** means data generated by Customer’s use of the Services or by Motorola Solutions’ support of the Services, including personal information, threat data, security threat intelligence and mitigation data, vulnerability data, threat scenarios, malicious and third-party IP information, malware, location, monitoring and recording activity, product performance and error information, threat signatures, activity logs and date and time of use.

2.7 **“Statement(s) of Work”** or **“SOW(s)”** as used in this Addendum means a statement of work, ordering document, accepted proposal, or other agreed upon engagement document issued under or subject to this Addendum. Mutually agreed upon SOWs may be attached hereto as Exhibit(s) A-1, A-2, A-3, etc., and/or are respectively incorporated by reference, each of which will be governed by the terms and conditions of this Addendum. Statements of Work may set out certain “Deliverables,” which include all written information (such as reports, specifications, designs, plans, drawings, or other technical or business information) that Motorola Solutions prepares for Customer in the performance of the Services and is obligated to provide to Customer under a SOW and this Addendum. The Deliverables, if any, are more fully described in the Statements of Work.

2.8 **“Third-Party Data”** means information obtained by Motorola Solutions from publicly available sources or its third-party content providers and made available to Customer through the products or Services.

Section 3. LICENSE, DATA AND SERVICE CONDITIONS

3.1 Delivery of Cyber Services

3.1.1 All Professional Services will be performed in accordance with the performance schedule included in a Statement of Work (SOW). Delivery of hours purchased as Retainer Services is at the onset of the applicable retainer period. Hours purchased as Retainer Services expire and are forfeited if not used within the Retainer period, subject to terms of use, expiration and extension, if any, as set out in the applicable SOW or ordering document. Professional Services described in a SOW will be deemed complete upon Motorola Solutions’ performance of such Services or, if applicable, upon exhaustion or expiration of the Retainer Services hours, whichever occurs first.

3.1.2 Subscription Services. Delivery of subscription services will occur upon Customer’s receipt of credentials required for access to the Services or upon Motorola Solutions otherwise providing access to the Services platform.

3.1.3 To the extent Customer purchases equipment from Motorola Solutions (“Supplied Equipment”), title and risk of loss to the Supplied Equipment will pass to Customer upon installation (if applicable) or shipment by Motorola Solutions. Customer will take all necessary actions, reimburse freight or delivery charges, provide or obtain access and other rights needed and take other requested actions necessary for Motorola Solutions to efficiently perform its contractual duties. To the extent Supplied Equipment is purchased on an installment basis, any early termination of the installment period will cause the outstanding balance to become immediately due.

3.2 Motorola Solutions may use or provide Customer with access to software, tools, enhancements, updates, data, derivative works, and other materials which Motorola Solutions has developed or licensed from third parties (collectively, “Motorola Solutions Materials”). The Services, Motorola Solutions Data, Third-Party Data, and related documentation, are considered Motorola Solutions Materials. Notwithstanding the use of such materials in Services or deliverables, the Motorola Solutions Materials are the property



of Motorola Solutions or its licensors, and Motorola Solutions or its licensors retain all right, title and interest in and to the Motorola Solutions Materials. Motorola Solutions grants Customer and Authorized Users a limited, non-transferable, non-sublicensable, and non-exclusive license to use the Services and associated deliverables solely for Customer's internal business purposes.

3.3 To the extent Customer is permitted to access, use, or integrate Customer or third-party software, services, content, or data that is not provided by Motorola Solutions (collectively, "Non-Motorola Solutions Content") with or through the Services, or will use equipment or software not provided by Motorola Solutions, which may be required for use of the Services ("Customer-Provided Equipment"), Customer will obtain and continuously maintain all rights and licenses necessary for Motorola Solutions to efficiently perform all contemplated Services under this Addendum and will assume responsibility for operation and integration of such content and equipment.

3.4 Ownership of Customer Data. Customer retains all right, title and interest, including intellectual property rights, if any, in and to Customer Data. Motorola Solutions acquires no rights to Customer Data except those rights granted under this Addendum including the right to Process and use the Customer Data as set forth in Section 3.5 – Processing Customer Data, below. The Parties agree that with regard to the Processing of personal information which may be part of Customer Data, Customer is the controller and Motorola Solutions is the processor, and Motorola Solutions may engage sub-processors pursuant to Section 3.5.3 – Sub-processors and Third-Party Providers.

3.5 Processing Customer Data.

3.5.1. Motorola Solutions Use of Customer Data. To the extent permitted by law, Customer grants Motorola Solutions and its subcontractors a right to use Customer Data and a royalty-free, worldwide, non-exclusive license to use Customer Data (including to process, host, cache, store, reproduce, copy, modify, combine, analyze, create derivative works from such Customer Data and to communicate, transmit, and distribute such Customer Data to third parties engaged by Motorola Solutions) to (a) perform Services and provide products under the Addendum, (b) analyze the Customer Data to operate, maintain, manage, and improve Motorola Solutions products and services, and (c) create new products and services. Customer agrees that this Addendum, along with any related documentation, are Customer's complete and final documented instructions to Motorola Solutions for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the change order process. Customer represents and warrants to Motorola Solutions that Customer's instructions, including appointment of Motorola Solutions as a processor or sub-processor, have been authorized by the relevant controller.

3.5.2 Collection, Creation, Use of Customer Data. Customer further represents and warrants that the Customer Data, Customer's collection, creation, and use of the Customer Data (including in connection with Motorola Solutions' Services), and Motorola Solutions' use of such Customer Data in accordance with the Addendum, will comply with all laws and will not violate any applicable privacy notices or infringe any third-party rights (including intellectual property and privacy rights). It is Customer's responsibility to obtain all required consents, provide all necessary notices, and meet any other applicable legal requirements with respect to collection and use (including Motorola Solutions' and third-party provider use) of the Customer Data as described in the Addendum or any applicable third-party agreements or EULAs.



3.5.3 Sub-processors and Third-Party Providers. Motorola Solutions may use, engage, resell, or otherwise interface with third-party software, hardware or services providers (such as, for example, third-party end point detection and response providers) and other sub-processors, who in turn may engage additional sub-processors to process personal data and other Customer Data. Customer agrees that such third-party software or services providers, sub-processors or their respective sub-processors may process and use personal and other Customer Data in accordance with and subject to their own respective licenses or terms and in accordance with applicable law. Customer authorizes and will provide and obtain all required notices and consents, if any, and comply with other applicable legal requirements, if any, with respect to such collection and use of personal data and other Customer Data by Motorola Solutions, and its subcontractors, sub-processors and/or third-party software, hardware or services providers. Notwithstanding any provision to the contrary, to the extent the use or performance of certain Services is governed by any separate license, data requirement, EULA, privacy statement, or other applicable agreement, including terms governing third-party software, hardware or services, including open source software, Customer will comply, and ensure its Authorized Users comply, with any such agreements or terms, which shall govern any such Services.

3.5.4 Notwithstanding any provision to the contrary in this Addendum or any related agreement, and in addition to other uses and rights set out herein, Customer understands and agrees that Motorola Solutions may obtain, use and/or create and use, anonymized, aggregated and/or generalized Customer Data, such as data relating to actual and potential security threats and vulnerabilities, for its lawful business purposes, including improving its services and sharing and leveraging such information for the benefit of Customer, other customers, and other interested parties.

3.6 Service Use Data. Customer understands and agrees that Motorola Solutions may collect and use Service Use Data for its own purposes, including the uses described below. Motorola Solutions may use Service Use Data to (a) operate, maintain, manage, improve existing and create new products and services, (b) test products and services, (c) to aggregate Service Use Data and combine it with that of other users, and (d) to use anonymized or aggregated data for marketing, research or other business purposes. Service Use Data may be disclosed to third parties. It is Customer's responsibility to notify Authorized Users of Motorola Solutions' collection and use of Service Use Data and to obtain any required consents, provide all necessary notices, and meet any other applicable legal requirements with respect to such collection and use, and Customer represents and warrants to Motorola Solutions that it has complied and will continue to comply with this Section.

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

3.8. Third-Party Data and Motorola Solutions Data. Motorola Solutions Data and Third-Party Data may be available to Customer through the Services. Customer will not, and will ensure its Authorized Users will not: (a) use the Motorola Solutions Data or Third-Party



Data for any purpose other than Customer's internal business purposes; (b) disclose the data to third parties; (c) "white label" such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (d) use such data in violation of applicable laws; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data; or (f) modify such data or combine it with Customer Data or other data or use the data to build databases. Any rights granted to Customer or Authorized Users with respect to Motorola Solutions Data or Third-Party Data will immediately terminate upon termination or expiration of this Addendum. Further, Motorola Solutions or the applicable Third-Party Data provider may suspend, change, or terminate Customer's or any Authorized User's access to Motorola Solutions Data or Third-Party Data if Motorola Solutions or such Third-Party Data provider believes Customer's or the Authorized User's use of the data violates the Addendum, applicable law or Motorola Solutions' agreement with the applicable Third-Party Data provider. Upon termination of Customer's rights to use any Motorola Solutions Data or Third-Party Data, Customer and all Authorized Users will immediately discontinue use of such data, delete all copies of such data, and certify such deletion to Motorola Solutions. Notwithstanding any provision of this Addendum and the Primary Agreement to the contrary, Motorola Solutions will have no liability for Third-Party Data or Motorola Solutions Data available through the Services. Motorola Solutions and its Third-Party Data providers reserve all rights in and to Motorola Solutions Data and Third-Party Data.

3.9 Customer will ensure its employees and Authorized Users comply with the terms of this Addendum and will be liable for all acts and omissions of its employees and Authorized Users. Customer is responsible for the secure management of Authorized Users' names, passwords and login credentials for access to products and Services. "Authorized Users" are Customer's employees, full-time contractors engaged for the purpose of supporting the products and Services that are not competitors of Motorola Solutions or its affiliates, and the entities (if any) specified in a SOW or otherwise approved by Motorola Solutions in writing (email from an authorized Motorola Solutions signatory accepted), which may include affiliates or other Customer agencies.

3.10 Motorola Solutions as a Controller or Joint Controller. In all instances where Motorola Solutions acts as a controller of data, it will comply with the applicable provisions of the Motorola Solutions Privacy Statement at https://www.motorolasolutions.com/en_us/about/privacy-policy.html#privacystatement, as may be updated from time to time. Motorola Solutions holds all Customer Contact Data as a controller and shall Process such Customer Contact Data in accordance with the Motorola Solutions Privacy Statement. In instances where Motorola Solutions is acting as a joint controller with Customer, the Parties will enter into a separate addendum to allocate the respective roles as joint controllers.

3.11 Beta or Proof of Concept Services. If Motorola Solutions makes any beta version of its Services ("Beta Service") available to Customer, or provides Customer a trial period or proof of concept period (or other demonstration) of the Services at reduced or no charge ("Proof of Concept" or "POC" Service), Customer may choose to use such Beta or POC Service at its own discretion, provided, however, that Customer will use the Beta or POC Service solely for purposes of Customer's evaluation of such Beta or POC Service, and for no other purpose. Customer acknowledges and agrees that all Beta or POC Services are offered "as-is" and without any representations or warranties or other commitments or protections from Motorola Solutions. Motorola Solutions will determine the duration of the evaluation period for any Beta or POC Service, in its sole discretion, and Motorola Solutions may discontinue any Beta or POC Service at any time. Customer acknowledges that Beta



Services, by their nature, have not been fully tested and may contain defects or deficiencies. Notwithstanding any other provision of this Agreement, to the extent a future paid Service has been agreed upon subject to and contingent on the Customer's evaluation of a Proof of Concept Service, Customer may cancel such future paid Service as specified in the SOW or, if not specified, within a reasonable time before the paid Service is initiated.

Section 4 WARRANTY

4.1 CUSTOMER ACKNOWLEDGES, UNDERSTANDS AND AGREES THAT MOTOROLA SOLUTIONS DOES NOT GUARANTEE OR WARRANT THAT IT WILL DISCOVER ALL OF CUSTOMER'S SECURITY EVENTS (SUCH EVENTS INCLUDING THE UNAUTHORIZED ACCESS, ACQUISITION, USE, DISCLOSURE, MODIFICATION OR DESTRUCTION OF CUSTOMER DATA), THREATS, OR SYSTEM VULNERABILITIES. MOTOROLA SOLUTIONS DISCLAIMS ANY AND ALL RESPONSIBILITY FOR ANY AND ALL LOSS OR COSTS OF ANY KIND ASSOCIATED WITH SECURITY EVENTS, THREATS OR VULNERABILITIES WHETHER OR NOT DISCOVERED BY MOTOROLA SOLUTIONS. MOTOROLA SOLUTIONS DISCLAIMS ANY RESPONSIBILITY FOR CUSTOMER'S 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. CUSTOMER SHALL BE RESPONSIBLE TO TAKE SUCH ACTIONS NECESSARY TO MITIGATE RISKS TO ITS OPERATIONS AND PROTECT AND PRESERVE ITS COMPUTER SYSTEMS AND DATA, INCLUDING CREATION OF OPERATIONAL WORKAROUNDS, BACKUPS AND REDUNDANCIES.

4.2. Customer acknowledges, understands and agrees that the Services and products or equipment provided by or used by Motorola Solutions to facilitate performance of the Services may impact or disrupt information systems. Motorola Solutions disclaims responsibility for costs in connection with any such disruptions of and/or damage to Customer's or a third party's information systems, equipment, voice transmissions, data and Customer Data, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision or delivery of the Service.

4.3. Motorola Solutions warrants that Supplied Equipment, under normal use and service, will be free from material defects in materials and workmanship for one (1) year from the date of shipment, subject to Customer providing written notice to Motorola Solutions within that period. AS IT RELATES TO THE SUPPLIED EQUIPMENT, MOTOROLA SOLUTIONS DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

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



Section 5 LIMITATION OF LIABILITY

5.1. DISCLAIMER OF CONSEQUENTIAL DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, MOTOROLA SOLUTIONS, ITS AFFILIATES, AND ITS AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, SUBCONTRACTORS, AGENTS, SUCCESSORS, AND ASSIGNS (COLLECTIVELY, THE "MOTOROLA SOLUTIONS PARTIES") WILL NOT BE LIABLE IN CONNECTION WITH THIS ADDENDUM (WHETHER UNDER MOTOROLA SOLUTIONS'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 SOLUTIONS 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.

5.2. DIRECT DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, THE TOTAL AGGREGATE LIABILITY OF THE MOTOROLA SOLUTIONS PARTIES, WHETHER BASED ON A CLAIM IN CONTRACT OR IN TORT, LAW OR EQUITY, RELATING TO OR ARISING OUT OF THIS ADDENDUM OR ANY RELATED OR UNDERLYING AGREEMENT, WILL NOT EXCEED THE FEES SET FORTH IN THE APPLICABLE SOW OR PRICING FOR THE CYBER SERVICES UNDER WHICH THE CLAIM AROSE. NOTWITHSTANDING THE FOREGOING, FOR ANY SUBSCRIPTION SERVICES OR FOR ANY RECURRING SERVICES, THE MOTOROLA SOLUTIONS PARTIES' TOTAL LIABILITY FOR ALL CLAIMS RELATED TO SUCH PRODUCT OR SERVICES IN THE AGGREGATE WILL NOT EXCEED THE TOTAL FEES PAID FOR THE CYBER SERVICES TO WHICH THE CLAIM IS RELATED DURING THE CONSECUTIVE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT FROM WHICH THE FIRST CLAIM AROSE. FOR AVOIDANCE OF DOUBT, THE LIMITATIONS IN THIS SECTION 5.2 APPLY IN THE AGGREGATE TO INDEMNIFICATION OBLIGATIONS ARISING OUT OF THIS ADDENDUM OR ANY RELATED AGREEMENTS.

5.3. ADDITIONAL EXCLUSIONS. NOTWITHSTANDING ANY OTHER PROVISION OF THIS ADDENDUM, THE PRIMARY AGREEMENT OR ANY RELATED AGREEMENT, MOTOROLA SOLUTIONS WILL HAVE NO LIABILITY FOR DAMAGES ARISING OUT OF (A) CUSTOMER DATA, INCLUDING ITS TRANSMISSION TO MOTOROLA SOLUTIONS, OR ANY OTHER DATA AVAILABLE THROUGH THE PRODUCTS OR SERVICES; (B) CUSTOMER-PROVIDED EQUIPMENT, NON-MOTOROLA SOLUTIONS CONTENT, THE SITES, OR THIRD-PARTY EQUIPMENT, HARDWARE, SOFTWARE, SERVICES, DATA, OR OTHER THIRD-PARTY MATERIALS, OR THE COMBINATION OF PRODUCTS AND SERVICES WITH ANY OF THE FOREGOING; (C) LOSS OF DATA OR HACKING, RANSOMWARE, OR OTHER THIRD-PARTY ATTACKS OR DEMANDS; (D) MODIFICATION OF PRODUCTS OR SERVICES BY ANY PERSON OTHER THAN MOTOROLA SOLUTIONS; (E) RECOMMENDATIONS PROVIDED IN CONNECTION WITH OR BY THE PRODUCTS AND SERVICES; (F) DATA RECOVERY SERVICES OR DATABASE MODIFICATIONS; OR (G) CUSTOMER'S OR ANY AUTHORIZED USER'S BREACH OF THIS ADDENDUM, THE PRIMARY AGREEMENT OR ANY RELATED AGREEMENT OR MISUSE OF THE PRODUCTS AND SERVICES; (H) INTERRUPTION OR FAILURE OF CONNECTIVITY, VULNERABILITIES, OR SECURITY EVENTS; (I) 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; (J) AVAILABILITY OR ACCURACY OF ANY DATA AVAILABLE THROUGH THE SERVICES,



OR INTERPRETATION, USE, OR MISUSE THEREOF; (K) TRACKING AND LOCATION-BASED SERVICES; OR (L) BETA SERVICES.

5.4. Voluntary Remedies. Motorola Solutions is not obligated to remedy, repair, replace, or refund the purchase price for the disclaimed issues in Section 5.3 – Additional Exclusions above, but if Motorola Solutions agrees to provide Services to help resolve such issues, Customer will reimburse Motorola Solutions for its reasonable time and expenses, including by paying Motorola Solutions any fees set forth in this Addendum or separate order for such Services, if applicable.

5.5. Representations and Standards. Except as expressly set out in this Addendum or the applicable Motorola Solutions proposal or statement of work relating to the cyber products or services, or applicable portion thereof, Motorola Solutions makes no representations as to the compliance of Motorola Solutions cyber products and services with any specific standards, specifications or terms. For avoidance of doubt, notwithstanding any related or underlying agreement or terms, conformance with any specific standards, specifications, or requirements, if any, as it relates to cyber products and services is only as expressly set out in the applicable Motorola Solutions SOW or proposal describing such cyber products or services or the applicable (i.e., cyber) portion thereof. Customer represents that it is authorized to engage Motorola Solutions to perform Services that may involve assessment, evaluation or monitoring of Motorola Solutions' or its affiliate's services, systems or products.

5.6. Wind Down of Services. In addition to any other termination rights, Motorola Solutions may terminate the Services, any SOW or subscription term, in whole or in part, in the event Motorola Solutions plans to cease offering the applicable Services to customers.

5.7. Third-Party Beneficiaries. The Addendum is entered into solely between, and may be enforced only by, the Parties. Each Party intends that the Addendum 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, products or services included in the Services will be a direct and intended third-party beneficiary of this Addendum.



EXHIBIT “D”

DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules and Annexes (“DPA”), forms part of the Primary Agreement entered into between the Parties (“Primary Agreement”) to reflect the parties’ agreement with regard to the Processing of Customer Data, which may include Personal Data. In the event of a conflict between this DPA, the Primary Agreement or any Schedule, Annex or other addenda to the Primary Agreement, this DPA must prevail.

When Customer renews or purchases new Products or Services, the then-current DPA must apply and must not change during the applicable Term. When Motorola provides new features or supplements the Product or Service, Motorola may provide additional terms or make updates to this DPA that must apply to Customer’s use of those new features or supplements.

1. Definitions.

All capitalized terms not defined herein must have the meaning set forth in the Agreement.

“**Customer Data**” means data including images, text, videos, and audio, that are provided to Motorola by, through, or on behalf of Customer and its Authorized Users or their end users, through the use of the Products and Services. Customer Data does not include Customer Contact Data, Service Use Data, other than that portion comprised of Personal Information, or Third Party Data.

“**Customer Contact Data**” means data Motorola collects from Customer, its Authorized Users, and their end users for business contact purposes, including without limitation marketing, advertising, licensing, and sales purposes.

“**Data Protection Laws**” means all data protection laws and regulations applicable to a Party with respect to the Processing of Personal Data under the Agreement.

“**Data Subjects**” means the identified or identifiable person to whom Personal Data relates.

“**Metadata**” means data that describes other data.

“**Motorola Data**” means data owned by Motorola and made available to Customer in connection with the Products and Services.

“**Personal Data**” or “**Personal Information**” means any information relating to an identified or identifiable natural person transmitted to Motorola by, through, or on behalf of Customer and its Authorized Users or their end users as part of Customer Data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one



or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Process” or “Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, copying, analyzing, caching, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Security Incident” means an incident leading to the accidental or unlawful destruction, loss, alteration or disclosure of, or access to Customer Data, which may include Personal Data, while processed by Motorola.

“Service Use Data” means data generated about the use of the Products and Services through Customer’s use or Motorola’s support of the Products and Services, which may include Metadata, Personal Data, product performance and error information, activity logs, and date and time of use.

“Sub-processor” means other processors engaged by Motorola to Process Customer Data which may include Personal Data.

“Third Party Data” means information obtained by Motorola from publicly available sources or its third party content providers and made available to Customer through the Products or Services.

2. Processing of Customer Data

2.1. Roles of the Parties. The Parties agree that with regard to the Processing of Personal Data hereunder, Customer is the Controller and Motorola is the Processor who may engage Sub-processors pursuant to the requirements of **Section 6** entitled “Sub-processors” below.

2.2. Motorola’s Processing of Customer Data. Motorola and Customer agree that Motorola may only use and Process Customer Data, including the Personal Information embedded in Service Use Data, in accordance with applicable law and Customer’s documented instructions for the following purposes: (i) to perform Services and provide Products under the Agreement; (ii) analyze Customer Data to operate, maintain, manage, and improve Motorola products and services; and (iii) create new products and services. Customer agrees that its Agreement (including this DPA), along with the Product and Service Documentation and Customer’s use and configuration of features in the Products and Services, are Customer’s complete and final documented instructions to Motorola for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer’s Agreement. Customer represents and warrants to Motorola that Customer’s instructions, including appointment of Motorola as a Processor or sub-processor, have been authorized by the relevant controller. Customer Data may be processed by Motorola at any of its global locations and/or disclosed to Subprocessors. It is Customer’s responsibility to notify Authorized Users of Motorola’s collection and use of Customer Data, and to obtain any required consents, provide all



necessary notices, and meet any other applicable legal requirements with respect to such collection and use. Customer represents and warrants to Motorola that it has complied with the terms of this provision.

2.3. Details of Processing. The subject-matter of Processing of Personal Data by Motorola hereunder, the duration of the Processing, the categories of Data Subjects and types of Personal Data are set forth on **Annex I** to this DPA.

2.4. Disclosure of Processed Data. Motorola must not disclose to or share any Customer Data with any third party except to Motorola's sub-processors, suppliers and channel partners as necessary to provide the products and services unless permitted under this Agreement, authorized by Customer or required by law. In the event a government or supervisory authority demands access to Customer Data, to the extent allowable by law, Motorola must provide Customer with notice of receipt of the demand to provide sufficient time for Customer to seek appropriate relief in the relevant jurisdiction. In all circumstances, Motorola retains the right to comply with applicable law. Motorola must ensure that its personnel are subject to a duty of confidentiality, and will contractually obligate its sub-processors to a duty of confidentiality, with respect to the handling of Customer Data and any Personal Data contained in Service Use Data.

2.5. Customer's Obligations. Customer is solely responsible for its compliance with all Data Protection Laws and establishing and maintaining its own policies and procedures to ensure such compliance. Customer must not use the Products and Services in a manner that would violate applicable Data Protection Laws. Customer must have sole responsibility for (i) the lawfulness of any transfer of Personal Data to Motorola, (ii) the accuracy, quality, and legality of Personal Data provided to Motorola; (iii) the means by which Customer acquired Personal Data, and (iv) the provision of any required notices to, and obtaining any necessary acknowledgements, authorizations or consents from Data Subjects. Customer takes full responsibility to keep the amount of Personal Data provided to Motorola to the minimum necessary for Motorola to perform in accordance with the Agreement. Customer must be solely responsible for its compliance with applicable Data Protection Laws.

2.6. Customer Indemnity. 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 Customer's failure to comply with its obligations under this Agreement and/or applicable Data Protection Laws. 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.

3. Service Use Data. Except to the extent that it is Personal Information, Customer understands and agrees that Motorola may collect and use Service Use Data for its own purposes, provided that such purposes are compliant with applicable Data Protection Laws. Service Use Data may be processed by Motorola at any of its global locations and/or disclosed to Subprocessors.

4. Third-Party Data and Motorola Data. Motorola Data and Third Party Data may be available to Customer through the Products and Services. Customer and its Authorized Users may use the Motorola Data and Third Party Data as permitted by Motorola and the applicable third-party data provider, as described in the Agreement or applicable Addendum. Unless expressly permitted in the Agreement or applicable Addendum, Customer must not, and must ensure its Authorized Users must not: (a) use the Motorola Data or Third-Party Data for any purpose other than Customer's internal business purposes or disclose the data to third parties; (b) "white label" such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (c) use such data in violation of applicable laws ; (d) use such data for activities or purposes where reliance upon the data could lead to death, injury, or property damage; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data; or (f) modify such data or combine it with Customer Data or other data or use the data to build databases. Additional restrictions may be set forth in the Agreement or applicable Addendum. Any rights granted to Customer or Authorized Users with respect to Motorola Data or Third-Party Data must immediately terminate upon termination or expiration of the applicable Addendum, Ordering Document, or the Primary Agreement. Further, Motorola or the applicable Third Party Data provider may suspend, change, or terminate Customer's or any Authorized User's access to Motorola Data or Third-Party Data if Motorola or such Third Party Data provider believes Customer's or the Authorized User's use of the data violates the Agreement, applicable law or by Motorola's agreement with the applicable Third Party Data provider. Upon termination of Customer's rights to use of any Motorola Data or Third-Party Data, Customer and all Authorized Users must immediately discontinue use of such data, delete all copies of such data, and certify such deletion to Motorola. Notwithstanding any provision of the Agreement to the contrary, Motorola has no liability for Third-Party Data or Motorola Data available through the Products and Services. Motorola and its Third Party Data providers reserve all rights in and to Motorola Data and Third-Party Data not expressly granted in an Addendum or Ordering Document.

5. Motorola as a Controller or Joint Controller. In all instances where Motorola acts as a Controller it must comply with the applicable provisions of the Motorola Privacy Statement at https://www.motorolasolutions.com/en_us/about/privacy-policy.html#privacystatement as each may be updated from time to time. Motorola holds all Customer Contact Data as a Controller and must Process such Customer Contact Data in accordance with the Motorola Privacy Statement. In instances where Motorola is acting as a Joint Controller with Customer, the Parties must enter into a separate addendum to the Agreement to allocate the respective roles as joint controllers.

6. Sub-processors.

6.1. Use of Sub-processors. Customer agrees that Motorola may engage Sub-processors who in turn may engage Sub-processors to Process Personal Data in accordance with the DPA. A current list of Sub-processors is set forth at **Annex III**. When engaging Sub-processors, Motorola must enter into agreements with the Sub-processors to bind them to obligations which are substantially similar or more stringent than those set out in this DPA.

6.2. Changes to Sub-processing. The Customer hereby consents to Motorola engaging Sub-processors to process Customer Data provided that: (i) Motorola must use its reasonable endeavours to provide at least 10 days' prior notice of the addition or removal of any Sub-processor, which may be given by posting details of such addition or removal at a URL provided to Customer in **Annex III**; (ii) Motorola imposes data protection terms on any Sub-processor it appoints that protect the Customer Data to the same standard provided for by this Addendum; and (iii) Motorola remains fully liable for any breach of this clause that is caused by an act, error or omission of its Sub-processor(s). The Customer may object to Motorola's appointment or replacement of a Sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Motorola will either appoint or replace the Sub-processor or, if in Motorola's discretion this is not feasible, the Customer may terminate this Agreement and receive a pro-rata refund of any prepaid service or support fees as full satisfaction of any claim arising out of such termination.

6.3. Data Subject Requests. Motorola must, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject, including without limitation requests for access to, correction, amendment, transport or deletion of such Data Subject's Personal Data and, to the extent applicable, Motorola must provide Customer with commercially reasonable cooperation and assistance in relation to any complaint, notice, or communication from a Data Subject. Customer must respond to and resolve promptly all requests from Data Subjects which Motorola provides to Customer. Customer must be responsible for any reasonable costs arising from Motorola's provision of such assistance under this Section.

7. Data Transfers

Motorola agrees that it must not make transfers of Personal Data under this Agreement from one jurisdiction to another unless such transfers are performed in compliance with this Addendum and applicable Data Protection Laws. Motorola agrees to enter into appropriate agreements with its affiliates and Sub-processors, which will permit Motorola to transfer Personal Data to its affiliates and Sub-processors. Motorola agrees to amend as necessary its agreement with Customer to permit transfer of Personal Data from Motorola to Customer. Motorola also agrees to assist the Customer in entering into agreements with its affiliates and Sub-processors if required by applicable Data Protection Laws for necessary transfers.

8. Security. Motorola must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the Processing of Personal Data, taking into account the costs of implementation; the nature, scope, context, and purposes of the Processing; and the risk of varying likelihood and severity of harm to the data subjects. The appropriate technical and organizational measures implemented by Motorola are set forth in **Annex III**. In assessing the appropriate level of security, Motorola must weigh the risks presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise Processed.

9. Security Incident Notification. If Motorola becomes aware of a Security Incident, then Motorola must (i) notify Customer of the Security Incident without undue delay, (ii) investigate



the Security Incident and apprise Customer of the details of the Security Incident and (iii) take commercially reasonable steps to stop any ongoing loss of Personal Data due to the Security Incident if in the control of Motorola. Notification of a Security Incident must not be construed as an acknowledgement or admission by Motorola of any fault or liability in connection with the Security Incident. Motorola must make reasonable efforts to assist Customer in fulfilling Customer's obligations under Data Protection Laws to notify the relevant supervisory authority and Data Subjects about such incident.

10. Data Retention and Deletion.

Except for anonymized Customer Data, as described above, or as otherwise provided under the Agreement, Motorola must delete all Customer Data no later than ninety (90) days following termination or expiration of the Primary Agreement or the applicable Addendum or Ordering Document unless otherwise required to comply with applicable law.

11. Audit Rights

11.1 Periodic Audit. Motorola will allow Customer to perform an audit of reasonable scope and duration of Motorola operations relevant to the Products and Services purchased under the Agreement, at Customer's sole expense, for verification of compliance with the technical and organizational measures set forth in **Annex II** if (i) Motorola notifies Customer of a Security Incident that results in actual compromise to the Products and/or Services purchased; or (ii) if Customer reasonably believes Motorola is not in compliance with its security commitments under this DPA, or (iii) if such audit is legally required by the Data Protection Laws. Any audit must be conducted in accordance with the procedures set forth in **Section 11.3** of this DPA and may not be conducted more than one time per year. If any such audit requires access to confidential information of Motorola's other customers, suppliers or agents, such portion of the audit may only be conducted by Customer's nationally recognized independent third party auditors in accordance with the procedures set forth in **Section 11.3** of this DPA. Unless mandated by GDPR or otherwise mandated by law or court order, no audits are allowed within a data center for security and compliance reasons. Motorola must, in no circumstances, provide Customer with the ability to audit any portion of its software, products, and services which would be reasonably expected to compromise the confidentiality of any third party's information or Personal Data.

11.2 Satisfaction of Audit Request. Upon receipt of a written request to audit, and subject to Customer's agreement, Motorola may satisfy such audit request by providing Customer with a confidential copy of a Motorola's applicable most recent third party security review performed by a nationally recognized independent third party auditor, such as a SOC2 Type II report or ISO 27001 certification, in order that Customer may reasonably verify Motorola's compliance with national standards.

11.3 Audit Process. Customer must provide at least sixty days (60) days prior written notice to Motorola of a request to conduct the audit described in **Section 11.1**. All audits must be conducted during normal business hours, at applicable locations or remotely, as designated by Motorola. Audit locations, if not remote will generally be those location(s) where Customer Data is accessed, or Processed. The audit must not unreasonably interfere with Motorola's



day to day operations. An audit must be conducted at Customer's sole cost and expense and subject to the terms of the confidentiality obligations set forth in the Agreement. Before the commencement of any such audit, Motorola and Customer must mutually agree upon the time, and duration of the audit. Motorola must provide reasonable cooperation with the audit, including providing the appointed auditor a right to review, but not copy, Motorola security information or materials provided such auditor has executed an appropriate non-disclosure agreement. Motorola's policy is to share methodology and executive summary information, not raw data or private information. Customer must, at no charge, provide to Motorola a full copy of all findings of the audit.

12. Regulation Specific Terms

12.1. HIPAA Business Associate. If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data as those terms are defined in 45 CFR § 160.103, execution of the Primary Agreement includes execution of the Motorola HIPAA Business Associate Agreement Addendum ("BAA"). Customer may opt out of the BAA by sending the following information to Motorola in a written notice under the terms of the Customer's Agreement: "Customer and Motorola agree that no Business Associate Agreement is required. Motorola is not a Business Associate of Customer's, and Customer agrees that it will not share or provide access to Protected Health Information to Motorola or Motorola's subprocessors."

12.2. FERPA. If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, Motorola acknowledges that for the purposes of the DPA, Motorola is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Motorola agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials. Customer understands that Motorola may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer must be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Motorola to students (or, with respect to a student under 18 years of age and not in attendance at a post-secondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Motorola's possession as may be required under applicable law.

12.3. CJIS. Motorola agrees to support the Customer's obligation to comply with the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy and must comply with the terms of the CJIS Security Addendum for the Term of this Agreement and such CJIS Security Addendum is incorporated herein by reference. Customer hereby consents to allow Motorola "screened" personnel as defined by the CJIS Security Policy to serve as an authorized "escort" within the meaning of CJIS Security Policy for escorting unscreened Motorola personnel that require access to unencrypted Criminal Justice Information for purposes of Tier 3 support (e.g. troubleshooting or development resources). In the event Customer requires access to Service Use Data for its compliance with the CJIS Security Policy, Motorola must make such access available following Customer's request. Notwithstanding the foregoing, in the event the Primary Agreement or applicable Ordering

Document terminates, Motorola must carry out deletion of Customer Data in compliance with Section 10 herein and may likewise delete Service Use Data within the time frame specified therein. To the extent Customer objects to deletion of its Customer Data or Service Use Data and seeks retention for a longer period, it must provide written notice to Motorola prior to expiration of the 30 day period for data retention to arrange return of the Customer Data and retention of the Service Use Data for a specified longer period of time.

12.4. CCPA / CPRA. If Motorola is Processing Personal Data within the scope of the California Consumer Protection Act (“CCPA”) and/or the California Privacy Rights Act (“CPRA”) (collectively referred to as the “California Privacy Acts”), Customer acknowledges that Motorola is a “Service Provider” within the meaning of California Privacy Acts. Motorola must process Customer Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the California Privacy Acts, including under any “sale” exemption. In no event will Motorola sell any such data, nor will M. If a California Privacy Act applies, Personal Data must also include any data identified with the California Privacy Act or Act’s definition of personal data. Motorola shall provide Customer with notice should it determine that it can no longer meet its obligations under the California Privacy Acts, and the parties agree that, if appropriate and reasonable, Customer may take steps necessary to stop and remediate unauthorized use of the impacted Personal Data.

12.5 CPA, CTDPA, VCDPA. If Motorola is Processing Personal Data within the scope of the Colorado Privacy Rights Act (“CPA”), the Connecticut Data Privacy Act (“CTDPA”), or the Virginia Consumer Data Protection Act (“VCDPA”) Motorola will comply with its obligations under the applicable legislation, and shall make available to Customer all information in its possession necessary to demonstrate compliance with obligations in accordance with such legislation. **Motorola Contact.** If Customer believes that Motorola is not adhering to its privacy or security obligations hereunder, Customer must contact the Motorola Data Protection Officer at Motorola Solutions, Inc., 500 W. Monroe, Chicago, IL USA 90661-3618 or at privacy1@motorolasolutions.com.

Motorola: Motorola Solutions, Inc.

Customer

By: _____

By:

Name: _____

Name:

Title: _____

Title:

Date: _____

Date:



ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1.

Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): Controller

2.

...

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1.

Name: Motorola Solutions, Inc.

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): Processor

2. ...



B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. Motorola acknowledges that, depending on Customer's use of the Online Service, Customer may elect to include personal data from any of the following types of data subjects in the Customer Data:

- Employees, contractors, and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of personal data transferred

Customer's use of the Products and Services, Customer may elect to include personal data from any of the following categories in the Customer Data:

- Basic personal data (for example place of birth, street name, and house number (address), Agreemental code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;



- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video, and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location, and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);



- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified under applicable law or regulation.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Data may be transferred on a continuous basis during the term of the Primary Agreement or other agreement to which this DPA applies.

Nature of the processing

The nature, scope and purpose of processing personal data is to carry out performance of Motorola's obligations with respect to provision of the Products and Services purchased under the Primary Agreement and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities

Purpose(s) of the data transfer and further processing

The nature, scope and purpose of processing personal data is to carry out performance of Motorola's obligations with respect to provision of the Products and Services purchased under the Primary Agreement and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period



Data retention is governed by Section 10 of this Data Processing Addendum

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Transfers to sub-processors will only be for carrying out the performance of Motorola's obligations with respect to provision of the Products and Services purchased under the Primary Agreement and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities. In accordance with the DPA, the data exporter agrees the data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such sub-processors must be permitted to obtain Customer Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data for any other purpose.



ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Measures of pseudonymisation and encryption of personal data

Where technically feasible and when not impacting services provided:

- We minimize the data we collect to information we believe is necessary to communicate, provide, and support products and services and information necessary to comply with legal obligations.
- We encrypt in transit and at rest.
- We pseudonymize and limit administrative accounts that have access to reverse pseudonymisation.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

In order to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services, Motorola Solutions Information Protection policy mandates the institutionalization of information protection throughout solution development and operational lifecycles. Motorola Solutions maintains dedicated security teams for its internal information security and its products and services. Its security practices and policies are integral to its business and mandatory for all Motorola Solutions employees and contractors. The Motorola Chief Information Security Officer maintains responsibility and executive oversight for such policies, including formal governance, revision management, personnel education and compliance. Motorola Solutions generally aligns to the NIST Cybersecurity Framework as well as ISO 27001.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Security Incident Procedures Motorola Solutions maintains a global incident response plan to address any physical or technical incident in an expeditious manner. Motorola maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. For each security breach that is a Security Incident, notification will be made in accordance with the Security Incident Notification section of this DPA.

Business Continuity and Disaster Preparedness Motorola maintains business continuity and disaster preparedness plans for critical functions and systems within Motorola's control that support the Products and Services purchased under the Agreement in order to avoid services disruptions and minimize recovery risks.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Motorola periodically evaluates its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with respect to the confidentiality, integrity, availability, and security of Customer Data, including personal information. Motorola documents the results of these evaluations and any remediation activities taken in response to such evaluations. Motorola periodically has third party assessments performed against applicable industry standards, such as ISO 27001, 27017, 27018 and 27701.

Measures for user identification and authorisation

Identification and Authentication. Motorola uses industry standard practices to identify and authenticate users who attempt to access Motorola information systems. Where authentication mechanisms are based on passwords, Motorola requires that the passwords are at least eight characters long and are changed regularly. Motorola uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Access Policy and Administration. Motorola maintains a record of security privileges of individuals having access to Customer Data, including personal information. Motorola maintains appropriate processes for requesting, approving and administering accounts and access privileges in connection with the Processing of Customer Data. Only authorized personnel may grant, alter or cancel authorized access to data and resources. Where an individual has access to systems containing Customer Data, the individuals are assigned separate, unique identifiers. Motorola deactivates authentication credentials on a periodic basis.

Measures for the protection of data during transmission

Data is generally encrypted during transmission within the Motorola managed environments. Encryption in transit is also generally required of any sub-processors. Further, protection of data in transit is also achieved through the access controls, physical and environmental security, and personnel security described throughout this Annex II.

Measures for the protection of data during storage

Data is generally encrypted during storage within the Motorola managed environments. Encryption in storage is also generally required of any sub-processors. Further, protection of data in storage is also achieved through the access controls, physical and environmental security, and personnel security described throughout this Annex II.

Measures for ensuring physical security of locations at which personal data are processed

Motorola maintains appropriate physical and environment security controls to prevent unauthorized access to Customer Data, including personal information. This includes appropriate physical entry controls to Motorola facilities such as card-controlled entry points, and a staffed reception desk to protect against unauthorized entry. Access to controlled areas within a facility will be limited by job role and subject to authorized approval. Use of an access badge to enter a controlled area will be logged and such logs will be retained in accordance with Motorola policy. Motorola revokes personnel access to Motorola facilities and controlled areas upon separation of employment in accordance with Motorola policies. Motorola policies impose industry standard workstation, device and media controls designed to further protect Customer Data, including personal information.

Measures for ensuring personnel security

Access to Customer Data. Motorola maintains processes for authorizing and supervising its employees, and contractors with respect to monitoring access to Customer Data. Motorola requires its employees, contractors and agents who have, or may be expected to have, access to Customer Data to comply with the provisions of the Agreement, including this Annex and any other applicable agreements binding upon Motorola.

Security and Privacy Awareness. Motorola must ensure that its employees and contractors remain aware of industry standard security and privacy practices, and their responsibilities for protecting Customer Data and Personal Data. This must include, but not be limited to, protection against malicious software, password protection, and management, and use of workstations and computer system accounts. Motorola requires periodic Information security training, privacy training, and business ethics training for all employees and contract resources

Sanction Policy. Motorola maintains a sanction policy to address violations of Motorola's internal security requirements as well as those imposed by law, regulation, or contract.

Background Checks. Motorola follows its standard mandatory employment verification requirements for all new hires. In accordance with Motorola internal policy, these requirements must be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation and any additional checks as deemed necessary by Motorola.

Measures for ensuring events logging

Protection, and Response. Motorola assesses organization's effectiveness annually via external assessors who report and share the assessment findings with Motorola Audit Services

who tracks any identified remediations. For more information, please see the Motorola Trust Center at https://www.motorolasolutions.com/en_us/about/trust-center/security.html

Measures for certification/assurance of processes and products

Motorola performs internal Secure Application Review and Secure Design Review security audits and Production Readiness Review security readiness reviews prior to service release. Where appropriate, privacy assessments are performed for Motorola's products and services. A risk register is created as a result of internal audits with assignments tasked to appropriate personnel. Security audits are performed annually with additional audits as needed. Additional privacy assessments, including updated data maps, occur when material changes are made to the products or services. Further, Motorola Solution has achieved AICPA SOC2 Type 2 reporting and ISO/IEC 27001:2013 certification for many of its development and support operations.

Measures for ensuring data minimisation

Motorola Solutions policies require processing of all personal information in accordance with applicable law, including when that law requires data minimisation. Further, Motorola Solutions conducts privacy assessments of its products and services and evaluates if those products and services support the principles of processing, such as data minimisation.

Measures for ensuring data quality

Motorola Solutions policies require processing of all personal information in accordance with applicable law, including when that law requires ensuring the quality and accuracy of data. Further, Motorola Solutions conducts privacy assessments of its products and services and evaluates if those products and services support the principles of processing, such as ensuring data quality.

Measures for ensuring limited data retention

Motorola Solutions maintains a data retention policy that provides a retention schedule outlining storage periods for personal data. The schedule is based on business needs and provides sufficient information to identify all records and to implement disposal decisions in line with the schedule. The policy is periodically reviewed and updated.

Measures for ensuring accountability

To ensure compliance with the principle of accountability, Motorola Solutions maintains a Privacy Program which generally aligns its activities to both the Nymity Privacy Management and Accountability Framework and NIST Privacy Framework. The Privacy Program is audited annually by Motorola Solutions Audit Services.

Measures for allowing data portability and ensuring erasure

When subject to a data subject request to move, copy or transfer their personal data, Motorola Solutions will provide personal data to the Controller in a structured, commonly used and machine readable format. Where possible and if the Controller requests it, Motorola Solutions can directly transmit the personal information to another organization.

For transfers to (sub-) processors

If, in the course of providing products and services under the Primary Agreement, Motorola Solutions transfers information containing personal data to third parties, said third parties will be subjected to a security assessment and bound by obligations substantially similar, but at least as stringent, as those included in this DPA.



ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors. The controller has authorised the use of the following sub-processors:

1.

Name: ...

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2.

...





East Bay Regional Communications System Authority



Participating agencies include Alameda and Contra Costa Counties and the following cities and special districts: Alameda, Albany, Antioch, Berkeley, Brentwood, Clayton, Concord, Danville, Dublin, El Cerrito, Emeryville, Fremont, Hayward, Hercules, Lafayette, Livermore, Martinez, Moraga, Newark, Oakley, Pinole, Pittsburg, Pleasant Hill, Pleasanton, Richmond, San Leandro, San Pablo, San Ramon, Union City, Walnut Creek, East Bay Regional Park District, Kensington Police Community Services District, Livermore Amador Valley Transit Authority, Moraga-Orinda Fire District, Rodeo-Hercules Fire District, San Ramon Valley Fire District, Ohlone Community College District, Contra Costa Community College District, Dublin-San Ramon Services District and University of California, Berkeley

BUDGET FISCAL YEAR 2023-24

Revenues

Operating payments	\$ 7,453,000
Service payments	1,512,000
Interest	100,000
Total revenues	9,065,000

Expenses

Administration	514,000
Audit fees	26,000
Contingency	100,000
Insurance	102,000
Lease	81,000
Legal	26,000
Licenses and permits	39,000
Membership fees	13,000
Maintenance	3,353,000
Security	33,000
Utilities	293,000
Website hosting	6,000
Total operating expenses	4,586,000
Capital	4,878,000
Debt Service	650,000
Total expenses	10,114,000
Net Income (Loss)	\$ (1,049,000)

Assumption: Operating payments 21,000 radio count at \$30 per month per radio
Service payments 8,400 radio count at \$15 per month per radio

EAST BAY REGIONAL COMMUNICATIONS SYSTEM AUTHORITY
EXPENDITURE DETAIL
FISCAL YEAR 2023-2024

OPERATING EXPENSES	FY22-23 Final Budget	FY22-23 Projected	FY23-24 Budget	Change FY23 vs FY24
Administration				
Executive director	\$ 263,000	\$ 237,040	\$ 263,000	\$ (25,960)
Administrative assistant	40,000	13,116	40,000	(26,884)
Training	-	-	30,000	(30,000)
Planning	134,000	-	161,000	(161,000)
Travel	5,000	300	7,000	(6,700)
Miscellaneous	10,000	164	13,000	(12,836)
Audit fees	20,000	17,820	26,000	(8,180)
Contingency	27,000	-	100,000	(100,000)
Insurance	75,000	72,168	102,000	(29,832)
Lease	73,000	69,050	81,000	(11,950)
Legal	20,000	11,009	26,000	(14,991)
Licenses and permits	30,000	-	39,000	(39,000)
Membership fees	10,000	9,194	13,000	(3,806)
Maintenance				
Service agreement	1,105,000	1,098,063	1,437,000	(338,937)
Software maintenance (SUA II)	985,000	978,249	-	978,249
Network administration	270,000	266,380	351,000	(84,620)
HVAC maintenance	57,000	55,792	75,000	(19,208)
Generator maintenance	53,000	33,779	69,000	(35,221)
ALCO general maintenance	600,000	600,000	660,000	(60,000)
COCO general maintenance	265,000	261,854	345,000	(83,146)
CSI telecommunications	200,000	40,000	260,000	(220,000)
Microwave maintenance	125,000	123,245	136,000	(12,755)
Miscellaneous	15,000	3,600	20,000	(16,400)
Security	25,000	21,900	33,000	(11,100)
Utilities	225,000	189,302	293,000	(103,698)
Website hosting	4,000	3,117	6,000	(2,883)
Total expenses	<u>4,636,000</u>	<u>4,105,142</u>	<u>4,586,000</u>	<u>(480,858)</u>
CAPITAL EXPENDITURES				
Walton Lane Simulcast Site	-	-	1,746,000	(1,746,000)
Microwave Network Upgrade	962,000	865,690	-	865,690
Encryption Upgrade	1,621,000	1,395,783	-	1,395,783
TDMA/Microwave Upgrade	1,664,000	1,663,030	1,872,000	(208,970)
DC Power Upgrade	250,000	-	250,000	(250,000)
Dispatch Consoles	25,000	-	25,000	(25,000)
Security System	30,000	29,496	-	29,496
Software maintenance (SUA II)	-	-	985,000	(985,000)
Total expenditures	<u>4,552,000</u>	<u>3,953,999</u>	<u>4,878,000</u>	<u>(924,001)</u>
DEBT SERVICE				
Principal	533,000	533,000	554,000	(21,000)
Interest	117,000	117,000	96,000	21,000
Total expenses	<u>\$ 650,000</u>	<u>\$ 650,000</u>	<u>\$ 650,000</u>	<u>\$ -</u>

1. TDMA Upgrade is the annual payment for the Change Order approved by the Board of Directors

2. DC Power Upgrade is an annual amount to replace the batteries in various locations

EAST BAY REGIONAL COMMUNICATIONS SYSTEM AUTHORITY
PROJECTED CASH RESERVE BALANCES
FISCAL YEAR 2023-2024

	FY22-23	FY22-23	FY23-24
	Final Budget	Projected	Budget
Operating Reserve			
Beginning Balance	\$ 1,904,000	\$ 1,904,000	\$ 2,052,500
Operating Payments	7,453,000	7,494,000	7,453,000
Initial Payments	-	18,000	-
Interest	100,000	176,000	100,000
Operating Expenses	(4,636,000)	(4,105,000)	(4,586,000)
Transfer to Capital Reserve	(2,502,503)	(3,434,500)	(3,726,500)
Ending Balance	2,318,497	2,052,500	1,293,000
Debt Service Reserve			
Beginning Balance	1,000,000	1,000,000	1,000,000
Service Payments	1,260,000	1,524,000	1,512,000
Debt Service	(650,000)	(650,000)	(650,000)
Transfer to Capital Reserve	(610,000)	(874,000)	(862,000)
Ending Balance	1,000,000	1,000,000	1,000,000
Capital Reserve			
Beginning Balance	12,693,000	12,693,000	13,047,500
Transfer In	3,112,503	4,308,500	4,588,500
Capital	(4,552,000)	(3,954,000)	(4,878,000)
Ending Balance	11,253,503	13,047,500	12,758,000
Total Reserve Balance	\$ 14,572,000	\$ 16,100,000	\$ 15,051,000

1. Operating Reserve Balance is equal to 50% of the next fiscal years Operating Budget
2. Debt Reserve Balance is set to equal \$1,000,000 every fiscal year
3. Capital Reserve Balance is the projected remaining cash after the Operating and Debt Reserve requirements have been met

EAST BAY REGIONAL COMMUNICATIONS SYSTEM AUTHORITY

10 YEAR CASH FLOW PROJECTION

	FY 2022-23	FY 2023-24	FY 2024-25	FY 2025-26	FY 2026-27	FY 2027-28	FY 2028-29	FY 2029-30	FY 2030-31	FY 2031-32
	Projected	Budget	Forecast	Forecast	Forecast	Forecast	Forecast	Forecast	Forecast	Forecast
Operating Reserve										
Balance - beginning	1,904,000	2,052,500	1,293,000	2,184,980	2,278,880	2,359,195	2,451,563	2,556,126	2,647,531	2,751,432
Receipts from members	7,688,000	7,553,000	7,660,000	7,660,000	7,660,000	7,660,000	7,660,000	7,660,000	7,660,000	7,660,000
Payments to suppliers	(4,105,000)	(4,586,000)	(4,369,960)	(4,557,760)	(4,718,390)	(4,903,126)	(5,112,252)	(5,295,062)	(5,502,863)	(5,736,661)
Transfer to Capital Reserve	(3,434,500)	(3,726,500)	(2,398,060)	(3,008,340)	(2,861,295)	(2,664,506)	(2,443,185)	(2,273,533)	(2,053,237)	(1,806,440)
Balance - ending	2,052,500	1,293,000	2,184,980	2,278,880	2,359,195	2,451,563	2,556,126	2,647,531	2,751,432	2,868,331
Debt Service Reserve										
Balance - beginning	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	-	-	-	-
Service payment	1,524,000	1,512,000	1,512,000	1,512,000	1,512,000	-	-	-	-	-
Principal	(533,000)	(554,000)	(576,000)	(600,000)	(623,000)	-	-	-	-	-
Bond interest	(117,000)	(96,000)	(74,000)	(50,000)	(27,000)	-	-	-	-	-
Transfer to Capital Reserve	(874,000)	(862,000)	(862,000)	(862,000)	(862,000)	(1,000,000)	-	-	-	-
Balance - ending	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	-	-	-	-	-
Capital Reserve										
Balance - beginning	12,693,000	13,047,500	12,758,000	12,871,660	13,554,624	14,047,928	14,438,123	13,560,905	14,338,099	14,845,143
Transfer In	4,308,500	4,588,500	3,260,060	3,870,340	3,723,295	3,664,506	2,443,185	2,273,533	2,053,237	1,806,440
Capital	(3,954,000)	(4,878,000)	(3,146,400)	(3,187,376)	(3,229,991)	(3,274,311)	(3,320,403)	(1,496,339)	(1,546,193)	(1,598,041)
Balance - ending	13,047,500	12,758,000	12,871,660	13,554,624	14,047,928	14,438,123	13,560,905	14,338,099	14,845,143	15,053,542
TOTAL RESERVE BALANCE	16,100,000	15,051,000	16,056,640	16,833,504	17,407,123	16,889,686	16,117,031	16,985,630	17,596,574	17,921,872

SUPPLEMENTARY SCHEDULE FOR PAYMENTS TO SUPPLIERS

Administration	(251,000)	(514,000)	(534,560)	(555,942)	(578,180)	(601,307)	(625,359)	(650,373)	(676,388)	(703,444)
Audit fees	(18,000)	(26,000)	(27,040)	(28,122)	(29,247)	(30,417)	(31,634)	(32,899)	(34,215)	(35,584)
Contingency	-	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)
Insurance	(72,000)	(102,000)	(106,080)	(110,323)	(114,736)	(119,325)	(124,098)	(129,062)	(134,224)	(139,593)
Legal	(11,000)	(26,000)	(27,040)	(28,122)	(29,247)	(30,417)	(31,634)	(32,899)	(34,215)	(35,584)
Lease	(69,000)	(81,000)	(84,240)	(87,610)	(91,114)	(94,759)	(98,549)	(102,491)	(106,591)	(110,855)
Licenses and permits	-	(39,000)	(40,560)	(42,182)	(43,869)	(45,624)	(47,449)	(49,347)	(51,321)	(53,374)
Membership fees	(9,000)	(13,000)	(13,520)	(14,061)	(14,623)	(15,208)	(15,816)	(16,449)	(17,107)	(17,791)
Maintenance										
Customer svc. agmt.	(1,098,000)	(1,437,000)	(1,099,000)	(1,142,960)	(1,188,678)	(1,236,225)	(1,285,674)	(1,337,101)	(1,390,585)	(1,446,208)
SUA II	(978,000)	-	-	-	-	-	-	-	-	-
System management	(266,000)	(351,000)	(365,040)	(379,642)	(394,828)	(410,621)	(427,046)	(444,128)	(461,893)	(480,369)
HVAC	(56,000)	(75,000)	(78,000)	(81,120)	(84,365)	(87,740)	(91,250)	(94,900)	(98,696)	(102,644)
Generators	(34,000)	(69,000)	(71,760)	(91,630)	(77,615)	(80,720)	(100,949)	(87,307)	(90,799)	(112,111)
ALCO maintenance	(600,000)	(660,000)	(686,400)	(713,856)	(742,410)	(772,106)	(802,990)	(835,110)	(868,514)	(903,255)
COCO maintenance	(262,000)	(345,000)	(358,800)	(373,152)	(388,078)	(403,601)	(419,745)	(436,535)	(453,996)	(472,156)
CSI	(40,000)	(260,000)	(270,400)	(281,216)	(292,465)	(304,164)	(316,331)	(328,984)	(342,143)	(355,829)
Microwave maintenance	(123,000)	(136,000)	(141,440)	(147,098)	(152,982)	(159,101)	(165,465)	(172,084)	(178,967)	(186,126)
Miscellaneous	(4,000)	(20,000)	(20,800)	(21,632)	(22,497)	(23,397)	(24,333)	(25,306)	(26,318)	(27,371)
Security	(22,000)	(33,000)	(34,320)	(35,693)	(37,121)	(38,606)	(40,150)	(41,756)	(43,426)	(45,163)
Utilities	(189,000)	(293,000)	(304,720)	(316,909)	(329,585)	(342,768)	(356,479)	(370,738)	(385,568)	(400,991)
Web site hosting	(3,000)	(6,000)	(6,240)	(6,490)	(6,750)	(7,020)	(7,301)	(7,593)	(7,897)	(8,213)
Payments to suppliers	(4,105,000)	(4,586,000)	(4,369,960)	(4,557,760)	(4,718,390)	(4,903,126)	(5,112,252)	(5,295,062)	(5,502,863)	(5,736,661)



East Bay Regional Communications System Authority



Participating agencies include Alameda and Contra Costa Counties and the following cities and special districts: Alameda, Albany, Antioch, Berkeley, Brentwood, Clayton, Concord, Danville, Dublin, El Cerrito, Emeryville, Fremont, Hayward, Hercules, Lafayette, Livermore, Martinez, Moraga, Newark, Oakley, Pinole, Pittsburg, Pleasant Hill, Pleasanton, Richmond, San Leandro, San Pablo, San Ramon, Union City, Walnut Creek, East Bay Regional Park District, Kensington Police Community Services District, Livermore Amador Valley Transit Authority, Moraga-Orinda Fire District, Rodeo-Hercules Fire District, San Ramon Valley Fire District, Ohlone Community College District, Contra Costa Community College District, Dublin-San Ramon Services District and University of California, Berkeley

BUDGET FISCAL YEAR 2023-24

Revenues

Operating payments	\$ 7,453,000
Service payments	1,512,000
Interest	100,000
Total revenues	<u>9,065,000</u>

Expenses

Administration	514,000
Audit fees	26,000
Contingency	100,000
Insurance	102,000
Lease	81,000
Legal	26,000
Licenses and permits	39,000
Membership fees	13,000
Maintenance	3,686,000
Security	33,000
Utilities	293,000
Website hosting	6,000
Total operating expenses	<u>4,919,000</u>
Capital	5,682,000
Debt Service	650,000
Total expenses	<u>11,251,000</u>
Net Income (Loss)	<u>\$ (2,186,000)</u>

Assumption: Operating payments 21,000 radio count at \$30 per month per radio
Service payments 8,400 radio count at \$15 per month per radio

**EAST BAY REGIONAL COMMUNICATIONS SYSTEM AUTHORITY
EXPENDITURE DETAIL
FISCAL YEAR 2023-2024**

OPERATING EXPENSES:	FY23-24 Approved	FY23-24 Amendment #1	FY23-24 Amended
Administrative			
Executive director	\$ 263,000		\$ 263,000
Administrative assistant	40,000		40,000
Training	30,000		30,000
Planning	161,000		161,000
Travel	7,000		7,000
Miscellaneous	13,000		13,000
Audit fees	26,000		26,000
Contingency	100,000		100,000
Insurance	102,000		102,000
Lease	81,000		81,000
Legal	26,000		26,000
Licenses and permit:	39,000		39,000
Membership fees	13,000		13,000
Maintenance			
Astro maintenance	-	1,479,000	1,479,000
MDR	-	291,000	291,000
Service agreement	1,437,000	(1,437,000)	-
Network administrative	351,000		351,000
HVAC maintenance	75,000		75,000
Generator maintenance	69,000		69,000
ALCO general maintenance	660,000		660,000
COCO general maintenance	345,000		345,000
CSI telecommunication:	260,000		260,000
Microwave maintenance	136,000		136,000
Miscellaneous	20,000		20,000
Security	33,000		33,000
Utilities:	293,000		293,000
Website hosting	6,000		6,000
Total expenses:	<u>4,586,000</u>	<u>333,000</u>	<u>4,919,000</u>
CAPITAL EXPENDITURES			
Astro SUA	-	1,369,000	1,369,000
MPLS	-	97,000	97,000
NICE SUA	-	323,000	323,000
Walton Lane Simulcast Site	1,746,000		1,746,000
TDMA/Microwave Upgrade	1,872,000		1,872,000
DC Power Upgrade	250,000		250,000
Dispatch Console:	25,000		25,000
Software maintenance (SUA II)	985,000	(985,000)	-
Total expenditure:	<u>4,878,000</u>	<u>804,000</u>	<u>5,682,000</u>
DEBT SERVICE			
Principal	554,000		554,000
Interest	96,000		96,000
Total expenses:	<u>\$ 650,000</u>	<u>\$ -</u>	<u>\$ 650,000</u>

1. TDMA Upgrade is the annual payment for the Change Order approved by the Board of Directors
2. DC Power Upgrade is an annual amount to replace the batteries in various locations

EAST BAY REGIONAL COMMUNICATIONS SYSTEM AUTHORITY
PROJECTED CASH RESERVE BALANCES
FISCAL YEAR 2023-2024

	FY22-23	FY22-23	FY23-24
	Final Budget	Actual	Budget
Operating Reserve			
Beginning Balance	\$ 1,904,000	\$ 1,904,000	\$ 1,946,163
Operating Payments	7,453,000	5,804,298	7,453,000
Initial Payments	-	18,000	-
Interest	100,000	198,683	100,000
Operating Expenses	(4,636,000)	(3,892,326)	(4,919,000)
Transfer to Capital Reserve	(2,502,503)	(2,086,492)	(3,120,663)
Ending Balance	2,318,497	1,946,163	1,459,500
Debt Service Reserve			
Beginning Balance	1,000,000	1,000,000	1,000,000
Service Payments	1,260,000	1,561,410	1,512,000
Debt Service	(650,000)	(648,802)	(650,000)
Transfer to Capital Reserve	(610,000)	(912,608)	(862,000)
Ending Balance	1,000,000	1,000,000	1,000,000
Capital Reserve			
Beginning Balance	12,693,000	12,693,000	13,281,904
Transfer In	3,112,503	2,999,100	3,982,663
Capital	(4,552,000)	(2,410,196)	(5,682,000)
Ending Balance	11,253,503	13,281,904	11,582,567
Total Reserve Balance	\$ 14,572,000	\$ 16,228,067	\$ 14,042,067

1. Operating Reserve Balance is equal to 50% of the next fiscal years Operating Budget. Per the recommendation of the Finance Committee, the Authority has transferred \$1 million of operating reserves to the capital reserve.
2. Debt Reserve Balance is set to equal \$1,000,000 every fiscal year
3. Capital Reserve Balance is the projected remaining cash after the Operating and Debt Reserve requirements have been met

EAST BAY REGIONAL COMMUNICATIONS SYSTEM AUTHORITY

10 YEAR CASH FLOW PROJECTION

	FY 2022-23	FY 2023-24	FY 2024-25	FY 2025-26	FY 2026-27	FY 2027-28	FY 2028-29	FY 2029-30	FY 2030-31	FY 2031-32	FY 2032-33
	Actual	Budget	Forecast	Forecast	Forecast	Forecast	Forecast	Forecast	Forecast	Forecast	Forecast
Operating Reserve											
Balance - beginning	1,904,000	1,946,163	1,459,500	2,555,294	2,664,006	2,759,753	2,868,146	2,989,375	3,098,110	3,220,034	3,355,677
Receipts from members	6,020,981	7,553,000	7,660,000	7,660,000	7,660,000	7,660,000	7,660,000	7,660,000	7,660,000	7,660,000	7,660,000
Payments to suppliers	(3,892,326)	(4,919,000)	(5,110,587)	(5,328,011)	(5,519,506)	(5,736,292)	(5,978,750)	(6,196,220)	(6,440,067)	(6,711,354)	(6,992,809)
Transfer to Capital Reserve	(2,086,492)	(3,120,663)	(1,453,620)	(2,223,277)	(2,044,747)	(1,815,315)	(1,560,021)	(1,355,045)	(1,098,009)	(813,003)	(526,464)
Balance - ending	1,946,163	1,459,500	2,555,294	2,664,006	2,759,753	2,868,146	2,989,375	3,098,110	3,220,034	3,355,677	3,496,404

Debt Service Reserve

Balance - beginning	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	-	-	-	-	-
Service payment	1,561,410	1,512,000	1,512,000	1,512,000	1,512,000	-	-	-	-	-	-
Principal	(532,000)	(554,000)	(576,000)	(600,000)	(623,000)	-	-	-	-	-	-
Bond interest	(116,802)	(96,000)	(74,000)	(50,000)	(27,000)	-	-	-	-	-	-
Transfer to Capital Reserve	(912,608)	(862,000)	(862,000)	(862,000)	(862,000)	(1,000,000)	-	-	-	-	-
Balance - ending	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	-	-	-	-	-	-

Capital Reserve

Balance - beginning	12,693,000	13,281,904	11,582,567	9,988,187	9,105,464	7,983,210	6,705,525	4,092,546	3,064,591	1,694,600	(49,397)
Transfer In	2,999,100	3,982,663	2,315,620	3,085,277	2,906,747	2,815,315	1,560,021	1,355,045	1,098,009	813,003	526,464
Capital	(2,410,196)	(5,682,000)	(3,910,000)	(3,968,000)	(4,029,000)	(4,093,000)	(4,173,000)	(2,383,000)	(2,468,000)	(2,557,000)	(2,649,000)
Balance - ending	13,281,904	11,582,567	9,988,187	9,105,464	7,983,210	6,705,525	4,092,546	3,064,591	1,694,600	(49,397)	(2,171,933)

TOTAL RESERVE BALANCE	16,228,067	14,042,067	13,543,480	12,769,469	11,742,963	9,573,671	7,081,921	6,162,701	4,914,634	3,306,280	1,324,471
------------------------------	-------------------	-------------------	-------------------	-------------------	-------------------	------------------	------------------	------------------	------------------	------------------	------------------

SUPPLEMENTARY SCHEDULE FOR PAYMENTS TO SUPPLIERS

Administration	(273,845)	(514,000)	(534,560)	(555,942)	(578,180)	(601,307)	(625,359)	(650,373)	(676,388)	(703,444)	(731,582)
Audit fees	(17,820)	(26,000)	(27,040)	(28,122)	(29,247)	(30,417)	(31,634)	(32,899)	(34,215)	(35,584)	(37,007)
Contingency	-	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)	(100,000)
Insurance	(72,168)	(102,000)	(106,080)	(110,323)	(114,736)	(119,325)	(124,098)	(129,062)	(134,224)	(139,593)	(145,177)
Legal	(14,694)	(26,000)	(27,040)	(28,122)	(29,247)	(30,417)	(31,634)	(32,899)	(34,215)	(35,584)	(37,007)
Lease	(69,050)	(81,000)	(84,240)	(87,610)	(91,114)	(94,759)	(98,549)	(102,491)	(106,591)	(110,855)	(115,289)
Licenses and permits	-	(39,000)	(40,560)	(42,182)	(43,869)	(45,624)	(47,449)	(49,347)	(51,321)	(53,374)	(55,509)
Membership fees	(9,194)	(13,000)	(13,520)	(14,061)	(14,623)	(15,208)	(15,816)	(16,449)	(17,107)	(17,791)	(18,503)
Maintenance											
Astro maintenance	-	(1,479,000)	(1,537,867)	(1,599,381)	(1,663,410)	(1,729,952)	(1,799,156)	(1,871,122)	(1,945,967)	(2,023,806)	(2,104,758)
MDR	-	(291,000)	(301,760)	(313,830)	(326,384)	(339,439)	(353,016)	(367,137)	(381,822)	(397,095)	(412,979)
Customer svc. agmt.	(1,098,062)	-	-	-	-	-	-	-	-	-	-
SUA II	(978,249)	-	-	-	-	-	-	-	-	-	-
System management	(266,380)	(351,000)	(365,040)	(379,642)	(394,828)	(410,621)	(427,046)	(444,128)	(461,893)	(480,369)	(499,584)
HVAC	(35,192)	(75,000)	(78,000)	(81,120)	(84,365)	(87,740)	(91,250)	(94,900)	(98,696)	(102,644)	(106,750)
Generators	(18,078)	(69,000)	(71,760)	(74,630)	(77,615)	(80,720)	(83,949)	(87,307)	(90,799)	(94,431)	(98,205)
ALCO maintenance	(600,000)	(660,000)	(686,400)	(713,856)	(742,410)	(772,106)	(802,990)	(835,110)	(868,514)	(903,255)	(939,385)
COCO maintenance	(176,425)	(345,000)	(358,800)	(373,152)	(388,078)	(403,601)	(419,745)	(436,535)	(453,996)	(472,156)	(491,042)
CSI	(19,913)	(260,000)	(270,400)	(281,216)	(292,465)	(304,164)	(316,331)	(328,984)	(342,143)	(355,829)	(370,062)
Microwave maintenance	(33,245)	(136,000)	(141,440)	(147,098)	(152,982)	(159,101)	(165,465)	(172,084)	(178,967)	(186,126)	(193,571)
Miscellaneous	(4,086)	(20,000)	(20,800)	(21,632)	(22,497)	(23,397)	(24,333)	(25,306)	(26,318)	(27,371)	(28,466)
Security	(21,144)	(33,000)	(34,320)	(35,693)	(37,121)	(38,606)	(40,150)	(41,756)	(43,426)	(45,163)	(46,970)
Utilities	(181,381)	(293,000)	(304,720)	(316,909)	(329,585)	(342,768)	(356,479)	(370,738)	(385,568)	(400,991)	(417,031)
Web site hosting	(3,400)	(6,000)	(6,240)	(6,490)	(6,750)	(7,020)	(7,301)	(7,593)	(7,897)	(8,213)	(8,542)
Payments to suppliers	(3,892,326)	(4,919,000)	(5,110,587)	(5,328,011)	(5,519,506)	(5,736,292)	(5,978,750)	(6,196,220)	(6,440,067)	(6,711,354)	(6,992,809)



**East Bay Regional
Communications
System Authority**



Participating agencies include Alameda and Contra Costa Counties and the following cities and special districts: Alameda, Albany, Antioch, Berkeley, Brentwood, Clayton, Concord, Danville, Dublin, El Cerrito, Emeryville, Fremont, Hayward, Hercules, Lafayette, Livermore, Martinez, Moraga, Newark, Oakley, Pinole, Pittsburg, Pleasant Hill, Pleasanton, Richmond, San Leandro, San Pablo, San Ramon, Union City, Walnut Creek, East Bay Regional Park District, Kensington Police Community Services District, Livermore Amador Valley Transit Authority, Moraga-Orinda Fire District, Rodeo-Hercules Fire District, San Ramon Valley Fire District, California Department of Transportation, Ohlone Community College District, Contra Costa Community College District, Dublin-San Ramon Services District and University of California, Berkeley

AGENDA ITEM 5.

**AGENDA STATEMENT
OPERATIONS COMMITTEE SPECIAL MEETING
MEETING DATE: September 15, 2023**

TO: Operations Committee
East Bay Regional Communications System Authority (EBRCSA)

FROM: Thomas G. McCarthy, Executive Director
East Bay Regional Communications System Authority

SUBJECT: Services Agreement with Contra Costa County Department of Information Technology

RECOMMENDATIONS:

Review, and if Committee agrees, make a recommendation to the Board of Directors to amend/extend an agreement with Contra Costa County Department of Information Technology to provide Communications Operations Support Services, radio services, installation, and maintenance of radio sites and 911 Dispatch centers that are part of the East Bay Regional Communications System Authority.

SUMMARY/DISCUSSION:

The Contra Costa County Department of Information Technology has a contract, attachment "B", with East Bay Regional Communications System Authority (EBRCSA) to provide radio services, installation, and maintenance of radio sites and 911 Dispatch centers that are part of EBRCSA. The current value of the contract, \$2,290,000, had been increased through amendments, attachment "B". Contra Costa County Department of Information Technology has requested the value of the contract be increased to \$2,635,000 and extended to June 30, 2024, attachment "A". The increase in the value of the contract over one year will be \$345,000. The amendment to the contract will allow them to perform work for EBRCSA until the contract

expires or is amended again in June 2024. Contra Costa County Department of Information Technology will continue to bill monthly for time and materials per the contract. The increase to the contract is necessary to compensate for the labor rates and cost of materials used performing the work.

FINANCIAL IMPACT:

The value of the contract had been increased through amendments and was \$2,290,000. Contra Costa County Department of Information Technology has requested the value of the contract be increased to \$2,635,000 and extended to June 30, 2024, see attachment “A”. The increase in the value of the contract over one year will be \$345,000. The approved FY 2023/2024 EBRCSA Budget has included \$345,000 for the Contra Costa County Department of Information Technology’s services.

The increase of the Services Agreement can be covered in projected operating revenue and will not require an increase in the user fees for EBRCSA members.

RECOMMENDED ACTION:

It is recommended the Committee make a recommendation to the Board of Directors that EBRCSA amend/extend its current contract with the Contra Costa County Department of Information Technology and increase the contract value from \$2,290,000, to \$2,635,000, an increase of \$345,000, through June 30, 2024.

The funding for the increase in the value of the contract is available in the maintenance budget.

Attachments:

Attachment “A” - Fiscal Year 2023 – 2024 Contract modification

Attachment “B” – Fiscal years 2021 – 2023 Contract Modification

Attachment “C” – Contract Contra Costa County Department of Information Technology

**CONTRACT AMENDMENT/EXTENSION
AGREEMENT
(Purchase of Services - Long Form)**

Number:
Fund/Org: 4285
Account: 2310
Other:

1. **Identification of Contract to be Extended.**

Number:

Effective Date: December 4, 2012

Department: Department of Information Technology

Subject: County provided radio services, installation, and maintenance of radio sites and 911 dispatch centers that are part of the East Bay Regional Communications System.

2. **Parties.** The County of Contra Costa, California (County), for its Department named above, and the following named Contractor mutually agree and promise as follows:

Contractor: East Bay Regional Communications System Authority

Capacity: California Joint Powers Authority

Address: 4985 Broder Blvd., Dublin, CA 94568

3. **Amendment Date.** The effective date of this Amendment/Extension Agreement is June 30, 2023.

4. **Amendment Specifications.** The Contract identified above is hereby amended as set forth in the "Amendment Specifications" attached hereto which are incorporated herein by reference. None

5. **Extension of Term.** The termination date of the above described contract is hereby extended from June 30, 2023 to a new termination date of June 30, 2024, unless sooner terminated as provided in said contract.

6. **Payment Limit Increase.** The payment limit of the above-described Contract is hereby increased by \$ 345,000, from \$ 2,290,000 to a new total Contract Payment Limit of \$ 2,635,000.


7. **Labor Service Rates.** EBRCSA will pay County \$148 per hour (the "Regular Rate") for work performed by a Communications Equipment Specialist between the hours of 8:00 a.m. and 5:00 p.m., Monday through Friday, excluding County holidays ("Regular Hours").

**CONTRACT AMENDMENT/EXTENSION
AGREEMENT
(Purchase of Services - Long Form)**

Number:
Fund/Org: 4285
Account: 2310
Other:

8. **Signatures.** These signatures attest the parties' agreement hereto:

COUNTY OF CONTRA COSTA, CALIFORNIA

BOARD OF SUPERVISORS	ATTEST: Clerk of the Board of Supervisors
By:  _____ Chair/Designee	By: _____ Deputy

CONTRACTOR

Signature A Name of business entity:	Signature B Name of business entity:
By: _____ (Signature of individual or officer)	By: _____ (Signature of individual or officer)
_____ (Print name and title A, if applicable)	_____ (Print name and title B, if applicable.)

Note to Contractor: For corporations (profit or nonprofit) and limited liability companies, the contract must be signed by two officers. Signature A must be that of the chairman of the board, president, or vice-president; and Signature B must be that of the secretary, any assistant secretary, chief financial officer or any assistant treasurer (Civil Code Section 1190 and Corporations Code Section 313). All signatures must be acknowledged as set forth on Form L-2.

**CONTRACT AMENDMENT/EXTENSION
AGREEMENT
(Purchase of Services – Long Form)**

Number:
Fund/Org:
Account:
Other:

1. **Identification of Contract to be Extended.**

Number:

Effective Date: December 4, 2012

Department: Department of Information Technology (DoIT)

Subject: County DoIT to provide radio services, installation and maintenance of radio sites and 911 Dispatch Centers that are part of the East Bay Regional Communications Systems.

2. **Parties.** The County of Contra Costa, California (County), for its Department named above, and the following named Contractor mutually agree and promise as follows:

Contractor: East Bay Regional Communications System Authority

Capacity: a California joint powers authority

Address: 4985 Broder Blvd., Dublin, CA 94568

3. **Amendment Date.** The effective date of this Amendment/Extension Agreement is June 30, 2021.

4. **Amendment Specifications.** The Contract identified above is hereby amended as set forth in the “Amendment Specifications” attached hereto which are incorporated herein by reference.

5. **Extension of Term.** The termination date of the above described contract is hereby extended from June 30, 2021 to a new termination date of June 30, 2023 , unless sooner terminated as provided in said contract.

6. **Payment Limit Increase.** The payment limit of the above described Contract is hereby increased by \$ 470,000, from \$ 1,820,000 to a new total Contract Payment Limit of \$ 2,290,000.

**CONTRACT AMENDMENT/EXTENSION
AGREEMENT
(Purchase of Services – Long Form)**

Number:
Fund/Org:
Account:
Other:

7. **Signatures.** These signatures attest the parties' agreement hereto:

COUNTY OF CONTRA COSTA, CALIFORNIA

BOARD OF SUPERVISORS By: _____ Chair/Designee	ATTEST: Clerk of the Board of Supervisors By: _____ Deputy
---	--

CONTRACTOR

Signature A Name of business entity: East Bay Regional Communications System Authority By: _____ (Signature of individual or officer) _____ (Print name and title A, if applicable)	Signature B Name of business entity: East Bay Regional Communications System Authority By: _____ (Signature of individual or officer) _____ (Print name and title B, if applicable.)
---	--

Note to Contractor: For corporations (profit or nonprofit) and limited liability companies, the contract must be signed by two officers. Signature A must be that of the chairman of the board, president, or vice-president; and Signature B must be that of the secretary, any assistant secretary, chief financial officer or any assistant treasurer (Civil Code Section 1190 and Corporations Code Section 313). All signatures must be acknowledged as set forth on Form L-2.

INTERAGENCY AGREEMENT
(County Provides Services)

1. **Contract Identification.**

Department: Department Of Information Technology (DoIT)

Subject: County DoIT to provide radio services, installations, and maintenance of radio sites and 911 Dispatch Centers that are part of the East Bay Regional Communications System.

2. **Parties.** The County of Contra Costa, California (County), for its Department named above, and the following named Agency mutually agree and promise as follows:

Agency: East Bay Regional Communications System Authority

Capacity: A California joint powers authority

Address: 4985 Broder Blvd. Dublin, CA 94568

3. **Term.** The effective date of this Agreement is December 4, 2012 and it terminates on December 3, 2015, unless sooner terminated as provided herein.

4. **Payment Limit.** Agency's total payments to County under this Agreement shall not exceed \$400,000.00.

5. **County's Obligations.** County shall provide those services and carry out that work described in the Service Plan attached hereto which is incorporated herein by reference, subject to all the terms and conditions contained or incorporated herein.

6. **Agency's Obligations.** Agency shall pay County for its provision of the services as set forth Section C of the Service Plan, and perform other obligations as specified in the Service Plan, subject to all the terms and conditions contained or incorporated herein.

7. **General and Special Conditions.** This Agreement is subject to the General Conditions and Special Conditions (if any) attached hereto, which are incorporated herein by reference.

8. **Project.** This Agreement implements in whole or in part the following described Project: East Bay Regional Communications System Authority communications project.

9. **Legal Authority.** This Agreement is entered into under and subject to the following legal authorities: Government Code Section 26227.

[Signatures appear on following page.]

10. **Signatures.** These signatures attest the parties' agreement hereto:

COUNTY OF CONTRA COSTA, CALIFORNIA

BOARD OF SUPERVISORS	ATTEST: Clerk of the Board of Supervisors
By: _____ Chairman/Designee	By: _____ Deputy

AGENCY

East Bay Regional Communications System Authority

Signature of authorized Agency representative	Signature of authorized Agency representative
By: <u>Gregory J. Ahern</u> Name: <u>Gregory J. Ahern</u> Title: <u>Alameda County Sheriff</u> <u>EBRCSA Board Chair</u>	By: <u>William J. McCammon</u> Name: <u>William J. McCammon</u> Title: <u>EBRCSA Executive Director</u>

ACKNOWLEDGMENT

STATE OF CALIFORNIA)
)
COUNTY OF CONTRA COSTA)

On _____, before me, _____
(insert name and title of the officer), personally appeared _____

_____ who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS MY HAND AND OFFICIAL SEAL.

Signature

(Seal)

ACKNOWLEDGMENT (by Corporation, Partnership, or Individual)
(Civil Code §1189)

APPROVALS

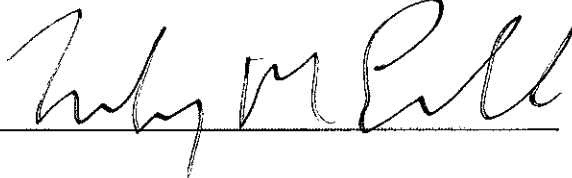
RECOMMENDED BY DEPARTMENT

FORM APPROVED
COUNTY COUNSEL

By: _____
Designee

By: _____
Deputy County Counsel
Eric Galston

APPROVED: COUNTY ADMINISTRATOR

By: 

Designee

1. **Payment Amounts.** Subject to the Payment Limit of this Contract and subject to the following Payment Provisions, County will pay Contractor the following fee as full compensation for all services, work, expenses or costs provided or incurred by Contractor:

[Check one alternative only.]

- a. \$ monthly, or
- b. \$ per unit, as defined in the Service Plan, or
- c. \$ after completion of all obligations and conditions herein.
- d. Other: As set forth in Section C of the Service Plan.
2. **Payment Demands.** Contractor shall submit written demands for payment on County Demand Form D-15 in the manner and form prescribed by County. Contractor shall submit said demands for payment no later than 30 days from the end of the month in which the contract services upon which such demand is based were actually rendered. Upon approval of payment demands by the head of the County Department for which this Contract is made, or his designee, County will make payments as specified in Paragraph 1. (Payment Amounts) above.
3. **Penalty for Late Submission.** If County is unable to obtain reimbursement from the State of California as a result of Contractor's failure to submit to County a timely demand for payment as specified in Paragraph 2. (Payment Demands) above, County shall not pay Contractor for such services to the extent County's recovery of funding is prejudiced by the delay even though such services were fully provided.
4. **Right to Withhold.** County has the right to withhold payment to Contractor when, in the opinion of County expressed in writing to Contractor, (a) Contractor's performance, in whole or in part, either has not been carried out or is insufficiently documented, (b) Contractor has neglected, failed or refused to furnish information or to cooperate with any inspection, review or audit of its program, work or records, or (c) Contractor has failed to sufficiently itemize or document its demand(s) for payment.

Initials: _____
Contractor County Dept.

5. **Audit Exceptions.** Contractor agrees to accept responsibility for receiving, replying to, and/or complying with any audit exceptions by appropriate county, state or federal audit agencies resulting from its performance of this Contract. Within 30 days of demand, Contractor shall pay County the full amount of County's obligation, if any, to the state and/or federal government resulting from any audit exceptions, to the extent such are attributable to Contractor's failure to perform properly any of its obligations under this Contract.

Initials: _____
Contractor County Dept.

SERVICE PLAN OUTLINE
(Purchase of Services - Long Form)

Number

SERVICE PLAN

A. County Obligations. County will provide the following services at East Bay Regional Communications System Authority ("EBRCSA") radio sites throughout Contra Costa County, and at the emergency operations center located in Dublin, Alameda County.

1. Installation and maintenance of P25 radio site land mobile radio hardware and software
2. Installation and maintenance services of microwave hardware and software.
3. Installation and maintenance of system and component monitoring equipment.
4. Installation and maintenance of radio site power supplies, generator, security systems, and other related equipment.
5. Installation, maintenance, planning, and engineering of radio shelter, tower or monopole, pathways, and related facilities.
6. Fleet map design, planning, training, and maintenance.
7. Site development services, which include site surveys, engineering, planning, coverage modeling, and specification development.
8. Installation and maintenance of dispatch consoles and console interface equipment.

With the prior written approval of EBRCSA, County may subcontract with third party service providers for the performance of services under this contract.

B. EBRCSA Obligations. EBRCSA will allow County to access its radio sites for the purpose of County performing the services called for under this contract.

C. Payment Provisions:

1. Labor Service Rates. County will be paid for its services according to the following hourly rates.
 - a. EBRCSA will pay County \$120 per hour (the "Regular Rate") for work performed by a Communications Equipment Specialist between the hours of 8:00 a.m. and 5:00 p.m., Monday through Friday, excluding County holidays ("Regular Hours").
 - b. EBRCSA will pay County at a rate equal to 1.5 times the Regular Rate for work performed by a Communications Equipment Specialist outside of Regular Hours.
 - c. County may increase the Regular Rate on an annual basis on July 1 of each year, but not in an amount in excess of five percent (5%) of the immediately preceding Regular Rate, and any such change will be effected by an amendment to this contract.
2. Materials and Third Party Vendor Charges. County will bill for materials used in performing services under this contract at its cost, and the materials will carry the manufacturer's warranty. County will bill for subcontractor services it uses to perform services under this contract at the cost any such third party service provider charges County.

Initials: _____
EBRCSA County

3. Invoices. County will submit said demands for payment no later than 60 days from the end of the month in which the contract services upon which such demand is based were actually rendered. EBRCSA will make payment in respect of invoices submitted within 30 days of receipt of an invoice.

Initials: _____
EBRCSA County

GENERAL CONDITIONS
(Purchase of Services - Long Form)

1. **Compliance with Law.** Contractor is subject to and must comply with all applicable federal, state, and local laws and regulations with respect to its performance under this Contract, including but not limited to, licensing, employment, and purchasing practices; and wages, hours, and conditions of employment, including nondiscrimination.

2. **Inspection.** Contractor's performance, place of business, and records pertaining to this Contract are subject to monitoring, inspection, review and audit by authorized representatives of the County, the State of California, and the United States Government.

3. **Records.** Contractor must keep and make available for inspection and copying by authorized representatives of the County, the State of California, and the United States Government, the Contractor's regular business records and such additional records pertaining to this Contract as may be required by the County.

a. **Retention of Records.** Contractor must retain all documents pertaining to this Contract for five years from the date of submission of Contractor's final payment demand or final Cost Report; for any further period that is required by law; and until all federal/state audits are complete and exceptions resolved for this Contract's funding period. Upon request, Contractor must make these records available to authorized representatives of the County, the State of California, and the United States Government.

b. **Access to Books and Records of Contractor, Subcontractor.** Pursuant to Section 1861(v)(1) of the Social Security Act, and any regulations promulgated thereunder, Contractor must, upon written request and until the expiration of five years after the furnishing of services pursuant to this Contract, make available to the County, the Secretary of Health and Human Services, or the Comptroller General, or any of their duly authorized representatives, this Contract and books, documents, and records of Contractor necessary to certify the nature and extent of all costs and charges hereunder.

Further, if Contractor carries out any of the duties of this Contract through a subcontract with a value or cost of \$10,000 or more over a twelve-month period, such subcontract must contain a clause to the effect that upon written request and until the expiration of five years after the furnishing of services pursuant to such subcontract, the subcontractor must make available to the County, the Secretary, the Comptroller General, or any of their duly authorized representatives, the subcontract and books,

Contractor

County Dept.

GENERAL CONDITIONS
(Purchase of Services - Long Form)

documents, and records of the subcontractor necessary to verify the nature and extent of all costs and charges thereunder.

This provision is in addition to any and all other terms regarding the maintenance or retention of records under this Contract and is binding on the heirs, successors, assigns and representatives of Contractor.

4. **Reporting Requirements.** Pursuant to Government Code Section 7550, Contractor must include in all documents and written reports completed and submitted to County in accordance with this Contract, a separate section listing the numbers and dollar amounts of all contracts and subcontracts relating to the preparation of each such document or written report. This section applies only if the Payment Limit of this Contract exceeds \$5,000.

5. **Termination and Cancellation.**

a. **Written Notice.** This Contract may be terminated by either party, in its sole discretion, upon thirty-day advance written notice thereof to the other, and may be cancelled immediately by written mutual consent.

b. **Failure to Perform.** County, upon written notice to Contractor, may immediately terminate this Contract should Contractor fail to perform properly any of its obligations hereunder. In the event of such termination, County may proceed with the work in any reasonable manner it chooses. The cost to County of completing Contractor's performance will be deducted from any sum due Contractor under this Contract, without prejudice to County's rights to recover damages.

c. **Cessation of Funding.** Notwithstanding any contrary language in Paragraphs 5 and 11, in the event that federal, state, or other non-County funding for this Contract ceases, this Contract is terminated without notice.

6. **Entire Agreement.** This Contract contains all the terms and conditions agreed upon by the parties. Except as expressly provided herein, no other understanding, oral or otherwise, regarding the subject matter of this Contract will be deemed to exist or to bind any of the parties hereto.

Contractor

County Dept.

GENERAL CONDITIONS
(Purchase of Services - Long Form)

7. Further Specifications for Operating Procedures. Detailed specifications of operating procedures and budgets required by this Contract, including but not limited to, monitoring, evaluating, auditing, billing, or regulatory changes, may be clarified in a written letter signed by Contractor and the department head, or designee, of the county department on whose behalf this Contract is made. No written clarification prepared pursuant to this Section will operate as an amendment to, or be considered to be a part of, this Contract.

8. Modifications and Amendments.

a. General Amendments. In the event that the Payment Limit of this Contract is \$100,000 or less, this Contract may be modified or amended only by a written document executed by Contractor and the County's Purchasing Agent or the Contra Costa County Board of Supervisors, subject to any required state or federal approval. In the event that the Payment Limit of this Contract exceeds \$100,000, this Contract may be modified or amended only by a written document executed by Contractor and the Contra Costa County Board of Supervisors or, after Board approval, by its designee, subject to any required state or federal approval.

b. Minor Amendments. The Payment Provisions and the Service Plan may be amended by a written administrative amendment executed by Contractor and the County Administrator (or designee), subject to any required state or federal approval, provided that such administrative amendment may not increase the Payment Limit of this Contract or reduce the services Contractor is obligated to provide pursuant to this Contract.

9. Disputes. Disagreements between County and Contractor concerning the meaning, requirements, or performance of this Contract shall be subject to final written determination by the head of the county department for which this Contract is made, or his designee, or in accordance with the applicable procedures (if any) required by the state or federal government.

10. Choice of Law and Personal Jurisdiction.

a. This Contract is made in Contra Costa County and is governed by, and must be construed in accordance with, the laws of the State of California.

Contractor

County Dept.

GENERAL CONDITIONS
(Purchase of Services - Long Form)

b. Any action relating to this Contract must be instituted and prosecuted in the courts of Contra Costa County, State of California.

11. Conformance with Federal and State Regulations and Laws. Should federal or state regulations or laws touching upon the subject of this Contract be adopted or revised during the term hereof, this Contract will be deemed amended to assure conformance with such federal or state requirements.

12. No Waiver by County. Subject to Paragraph 9. (Disputes) of these General Conditions, inspections or approvals, or statements by any officer, agent or employee of County indicating Contractor's performance or any part thereof complies with the requirements of this Contract, or acceptance of the whole or any part of said performance, or payments therefor, or any combination of these acts, do not relieve Contractor's obligation to fulfill this Contract as prescribed; nor is the County thereby prevented from bringing any action for damages or enforcement arising from any failure to comply with any of the terms and conditions of this Contract.

13. Subcontract and Assignment. This Contract binds the heirs, successors, assigns and representatives of Contractor. Prior written consent of the County Administrator or his designee, subject to any required state or federal approval, is required before the Contractor may enter into subcontracts for any work contemplated under this Contract, or before the Contractor may assign this Contract or monies due or to become due, by operation of law or otherwise.

14. Independent Contractor Status. The parties intend that Contractor, in performing the services specified herein, is acting as an independent contractor and that Contractor will control the work and the manner in which it is performed. This Contract is not to be construed to create the relationship between the parties of agent, servant, employee, partnership, joint venture, or association. Additionally, Contractor is not entitled to participate in any pension plan, workers' compensation plan, insurance, bonus, or similar benefits County provides to its employees. In the event that County exercises its right to terminate this Contract, Contractor expressly agrees that it will have no recourse or right of appeal under any rules, regulations, ordinances, or laws applicable to employees.

15. Conflicts of Interest. Contractor covenants that it presently has no interest and that it will not acquire any interest, direct or indirect, that represents a financial conflict of interest under state law or that would otherwise conflict in any manner or degree with the performance of its services hereunder. Contractor further covenants that in the performance of this Contract, no person having any such interests will be

Contractor

County Dept.

GENERAL CONDITIONS
(Purchase of Services - Long Form)

employed by Contractor. If requested to do so by County, Contractor will complete a "Statement of Economic Interest" form and file it with County and will require any other person doing work under this Contract to complete a "Statement of Economic Interest" form and file it with County. Contractor covenants that Contractor, its employees and officials, are not now employed by County and have not been so employed by County within twelve months immediately preceding this Contract; or, if so employed, did not then and do not now occupy a position that would create a conflict of interest under Government Code section 1090. In addition to any indemnity provided by Contractor in this Contract, Contractor will indemnify, defend, and hold the County harmless from any and all claims, investigations, liabilities, or damages resulting from or related to any and all alleged conflicts of interest.

16. **Confidentiality.** Contractor agrees to comply and to require its officers, partners, associates, agents and employees to comply with all applicable state or federal statutes or regulations respecting confidentiality, including but not limited to, the identity of persons served under this Contract, their records, or services provided them, and assures that:

- a. All applications and records concerning any individual made or kept by Contractor or any public officer or agency in connection with the administration of or relating to services provided under this Contract will be confidential, and will not be open to examination for any purpose not directly connected with the administration of such service.
- b. No person will publish or disclose or permit or cause to be published or disclosed, any list of persons receiving services, except as may be required in the administration of such service. Contractor agrees to inform all employees, agents and partners of the above provisions, and that any person knowingly and intentionally disclosing such information other than as authorized by law may be guilty of a misdemeanor.

17. **Nondiscriminatory Services.** Contractor agrees that all goods and services under this Contract will be available to all qualified persons regardless of age, gender, race, religion, color, national origin, ethnic background, disability, or sexual orientation, and that none will be used, in whole or in part, for religious worship.

18. **Indemnification.** Contractor will defend, indemnify, save, and hold harmless County and its officers and employees from any and all claims, demands, losses, costs, expenses, and liabilities for any damages, fines, sickness, death, or injury to person(s) or property, including any and all administrative fines,

Contractor

County Dept.

GENERAL CONDITIONS
(Purchase of Services - Long Form)

penalties or costs imposed as a result of an administrative or quasi-judicial proceeding, arising directly or indirectly from or connected with the services provided hereunder that are caused, or claimed or alleged to be caused, in whole or in part, by the negligence or willful misconduct of Contractor, its officers, employees, agents, contractors, subcontractors, or any persons under its direction or control. If requested by County, Contractor will defend any such suits at its sole cost and expense. If County elects to provide its own defense, Contractor will reimburse County for any expenditures, including reasonable attorney's fees and costs. Contractor's obligations under this section exist regardless of concurrent negligence or willful misconduct on the part of the County or any other person; provided, however, that Contractor is not required to indemnify County for the proportion of liability a court determines is attributable to the sole negligence or willful misconduct of the County, its officers and employees. This provision will survive the expiration or termination of this Contract.

19. **Insurance.** During the entire term of this Contract and any extension or modification thereof, Contractor shall keep in effect insurance policies meeting the following insurance requirements unless otherwise expressed in the Special Conditions:

a. **Commercial General Liability Insurance.** For all contracts where the total payment limit of the contract is \$500,000 or less, Contractor will provide commercial general liability insurance, including coverage for business losses and for owned and non-owned automobiles, with a minimum combined single limit coverage of \$500,000 for all damages, including consequential damages, due to bodily injury, sickness or disease, or death to any person or damage to or destruction of property, including the loss of use thereof, arising from each occurrence. Such insurance must be endorsed to include County and its officers and employees as additional insureds as to all services performed by Contractor under this Contract. Said policies must constitute primary insurance as to County, the state and federal governments, and their officers, agents, and employees, so that other insurance policies held by them or their self-insurance program(s) will not be required to contribute to any loss covered under Contractor's insurance policy or policies. For all contracts where the total payment limit is greater than \$500,000, the aforementioned insurance coverage to be provided by Contractor must have a minimum combined single limit coverage of \$1,000,000, and Contractor must provide County with a copy of the endorsement making the County an additional insured on all commercial general liability, worker's compensation, and, if applicable, all professional liability insurance policies as required herein no later than the effective date of this Contract.

Contractor

County Dept.

GENERAL CONDITIONS
(Purchase of Services - Long Form)

b. Workers' Compensation. Contractor must provide workers' compensation insurance coverage for its employees.

c. Certificate of Insurance. The Contractor must provide County with (a) certificate(s) of insurance evidencing liability and worker's compensation insurance as required herein no later than the effective date of this Contract. If Contractor should renew the insurance policy(ies) or acquire either a new insurance policy(ies) or amend the coverage afforded through an endorsement to the policy at any time during the term of this Contract, then Contractor must provide (a) current certificate(s) of insurance.

d. Additional Insurance Provisions. The insurance policies provided by Contractor must include a provision for thirty (30) days written notice to County before cancellation or material change of the above-specified coverage.

20. Notices. All notices provided for by this Contract must be in writing and may be delivered by deposit in the United States mail, postage prepaid. Notices to County must be addressed to the head of the county department for which this Contract is made. Notices to Contractor must be addressed to the Contractor's address designated herein. The effective date of notice is the date of deposit in the mails or of other delivery, except that the effective date of notice to County is the date of receipt by the head of the county department for which this Contract is made.

21. Primacy of General Conditions. In the event of a conflict between the General Conditions and the Special Conditions, the General Conditions govern unless the Special Conditions or Service Plan expressly provide otherwise.

22. Nonrenewal. Contractor understands and agrees that there is no representation, implication, or understanding that the services provided by Contractor under this Contract will be purchased by County under a new contract following expiration or termination of this Contract, and Contractor waives all rights or claims to notice or hearing respecting any failure to continue purchasing all or any such services from Contractor.

23. Possessory Interest. If this Contract results in Contractor having possession of, claim or right to the possession of land or improvements, but does not vest ownership of the land or improvements in the same

Contractor

County Dept.

GENERAL CONDITIONS
(Purchase of Services - Long Form)

person, or if this Contract results in the placement of taxable improvements on tax exempt land (Revenue & Taxation Code Section 107), such interest or improvements may represent a possessory interest subject to property tax, and Contractor may be subject to the payment of property taxes levied on such interest. Contractor agrees that this provision complies with the notice requirements of Revenue & Taxation Code Section 107.6, and waives all rights to further notice or to damages under that or any comparable statute.

24. **No Third-Party Beneficiaries.** Nothing in this Contract may be construed to create, and the parties do not intend to create, any rights in third parties.

25. **Copyrights and Rights in Data.** Contractor will not publish or transfer any materials produced or resulting from activities supported by this Contract without the express written consent of the County Administrator. If any material is subject to copyright, County reserves the right to copyright, and Contractor agrees not to copyright such material. If the material is copyrighted, County reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, and use such materials, in whole or in part, and to authorize others to do so.

26. **Endorsements.** In its capacity as a contractor with Contra Costa County, Contractor will not publicly endorse or oppose the use of any particular brand name or commercial product without the prior written approval of the Board of Supervisors. In its County-contractor capacity, Contractor will not publicly attribute qualities or lack of qualities to a particular brand name or commercial product in the absence of a well-established and widely accepted scientific basis for such claims or without the prior written approval of the Board of Supervisors. In its County-contractor capacity, Contractor will not participate or appear in any commercially produced advertisements designed to promote a particular brand name or commercial product, even if Contractor is not publicly endorsing a product, as long as the Contractor's presence in the advertisement can reasonably be interpreted as an endorsement of the product by or on behalf of Contra Costa County. Notwithstanding the foregoing, Contractor may express its views on products to other contractors, the Board of Supervisors, County officers, or others who may be authorized by the Board of Supervisors or by law to receive such views.

27. **Required Audit.** (A) If Contractor is funded by \$500,000 or more in federal grant funds in any fiscal year from any source, Contractor must provide to County, at Contractor's expense, an audit conforming to the requirements set forth in the most current version of Office of Management and Budget Circular A-133. (B) If Contractor is funded by less than \$500,000 in federal grant funds in any fiscal year from any source, but such grant imposes specific audit requirements, Contractor must

Contractor

County Dept.

GENERAL CONDITIONS
(Purchase of Services - Long Form)

provide County with an audit conforming to those requirements. (C) If Contractor is funded by less than \$500,000 in federal grant funds in any fiscal year from any source, Contractor is exempt from federal audit requirements for that year; however, Contractor's records must be available for and an audit may be required by, appropriate officials of the federal awarding agency, the General Accounting Office (GAO), the pass-through entity and/or the County. If any such audit is required, Contractor must provide County with such audit. With respect to the audits specified in (A), (B) and (C) above, Contractor is solely responsible for arranging for the conduct of the audit, and for its cost. County may withhold the estimated cost of the audit or 10 percent of the contract amount, whichever is greater, or the final payment, from Contractor until County receives the audit from Contractor.

28. Authorization. Contractor, or the representative(s) signing this Contract on behalf of Contractor, represents and warrants that it has full power and authority to enter into this Contract and to perform the obligations set forth herein.

29. No Implied Waiver. The waiver by County of any breach of any term or provision of this Contract will not be deemed to be a waiver of such term or provision or of any subsequent breach of the same or any other term or provision contained herein.

Contractor

County Dept.

SPECIAL CONDITIONS
(Purchase of Services - Long Form)

The following Special Conditions are hereby made part of the contract between Contra Costa County, and East Bay Regional Communications System Authority, a California Joint Powers Authority ("EBRCSA").

1. References in these Special Conditions to "Contractor" are deemed to be references to Contra Costa County, on behalf of its Department of Information Technology.

2. The General Conditions attached to this contract are hereby deleted in their entirety and replaced with the following:

"1. Compliance with Law. Each of Contractor and County are subject to and must comply with all applicable federal, state, and local laws and regulations with respect to its performance under this Contract, including but not limited to, licensing, employment, and purchasing practices; and wages, hours, and conditions of employment, including nondiscrimination.

2. Inspection. Contractor's performance, place of business, and records pertaining to this Contract are subject to monitoring, inspection, review and audit by authorized representatives of EBRCSA.

3. Records. Contractor must keep and make available for inspection and copying by authorized representatives of EBRCSA, the State of California, and the United States Government, the Contractor's regular business records and such additional records pertaining to this Contract as may be required by EBRCSA.

4. Termination and Cancellation. This Contract may be terminated by either party, in its sole discretion, upon thirty-day advance written notice thereof to the other, and may be cancelled immediately by written mutual consent.

5. Entire Agreement. This Contract contains all the terms and conditions agreed upon by the parties. Except as expressly provided herein, no other understanding, oral or otherwise, regarding the subject matter of this Contract will be deemed to exist or to bind any of the parties hereto.

6. Further Specifications for Operating Procedures. Detailed specifications of operating procedures and budgets required by this Contract, including but not limited to, monitoring, evaluating, auditing, billing, or regulatory changes, may be clarified in a written letter signed by EBRCSA and the department head, or designee, of the county department on whose behalf this Contract is made. No written clarification prepared pursuant to this Section will operate as an amendment to, or be considered to be a part of, this Contract.

7. Modifications and Amendments. This Contract may be modified or amended only by a written document executed by EBRCSA and the Contra Costa County Board of Supervisors or, after

Initials:

EBRCSA

County

Board approval, by its designee, subject to any required state or federal approval.

8. Disputes. Disagreements between EBRCSA y and Contractor concerning the meaning, requirements, or performance of this Contract shall be subject to final written determination by the head of the county department for which this Contract is made, or his or her designee, or in accordance with the applicable procedures (if any) required by the state or federal government.

9. Choice of Law and Personal Jurisdiction.

a. This Contract is made in Contra Costa County and is governed by, and must be construed in accordance with, the laws of the State of California.

b. Any action relating to this Contract must be instituted and prosecuted in the courts of Contra Costa County, State of California.

10. Conformance with Federal and State Regulations and Laws. Should federal or state regulations or laws touching upon the subject of this Contract be adopted or revised during the term hereof, this Contract will be deemed amended to assure conformance with such federal or state requirements.

11. No Waiver by EBRCSA. Subject to Paragraph 8. (Disputes) of these Special Conditions, inspections or approvals, or statements by any officer, agent or employee of Contractor indicating Contractor's performance or any part thereof complies with the requirements of this Contract, or acceptance of the whole or any part of said performance, or payments therefor, or any combination of these acts, do not relieve Contractor's obligation to fulfill this Contract as prescribed; nor is EBRCSA thereby prevented from bringing any action for damages or enforcement arising from any failure to comply with any of the terms and conditions of this Contract.

12. Subcontract and Assignment. This Contract binds the heirs, successors, assigns and representatives of Contractor. Neither party may assign this Contract without the prior written approval of the other party.

13. Independent Contractor Status. This Contract is not to be construed to create the relationship between the parties of agent, servant, employee, partnership, joint venture, or association, and Contractor shall have no entitlement to participate in any pension plan, workers' compensation plan, insurance, bonus, or similar benefits provided by EBRCSA to its employees (if any), agents, officers, consultants or volunteers. In the event that EBRCSA exercises its right to terminate this Contract, Contractor expressly agrees that it will have no recourse or right of appeal under any rules, regulations, ordinances, or laws applicable to employees.

14. Conflicts of Interest. Contractor covenants that it presently has no interest and that it will not acquire any interest, direct or indirect, that represents a financial conflict of interest under state law or that would otherwise conflict in any manner or degree with the performance of its services hereunder. Contractor further covenants that in the performance of this Contract, no person having any such interests will be employed by Contractor. If requested to do so by EBRCSA, Contractor will complete a "Statement of Economic Interest" form and file it with EBRCSA and will require any other person doing work under this Contract to complete a "Statement of Economic Interest" form and file it with EBRCSA.

Initials: _____
EBRCSA County

15. Confidentiality. Contractor agrees to comply and to require its officers, partners, associates, agents and employees to comply with all applicable state or federal statutes or regulations respecting confidentiality, including but not limited to, the identity of persons served under this Contract, their records, or services provided them.

16. Nondiscriminatory Services. Contractor agrees that all goods and services under this Contract will be available to all qualified persons regardless of age, gender, race, religion, color, national origin, ethnic background, disability, or sexual orientation.

17. Indemnification.

a. Contractor Indemnification. Contractor will defend, indemnify, save, and hold harmless EBRCSA and its officers, agents and employees, if any, from any and all claims, demands, losses, costs, expenses, and liabilities for any damages, fines, sickness, death, or injury to person(s) or property, including any and all administrative fines, penalties or costs imposed as a result of an administrative or quasi-judicial proceeding, arising directly or indirectly from or connected with the services provided hereunder that are caused, or claimed or alleged to be caused, in whole or in part, by the negligence or willful misconduct of Contractor, its officers, employees, agents, contractors, subcontractors, or any persons under its direction or control. If requested by EBRCSA, Contractor will defend any such suits at its sole cost and expense. If EBRCSA elects to provide its own defense, Contractor will reimburse EBRCSA for any expenditures, including reasonable attorneys' fees and costs. Contractor is not required to indemnify EBRCSA for the proportion of liability a court determines is attributable to the negligence or willful misconduct of EBRCSA, its officers, agents and employees, if any. This provision will survive the expiration or termination of this Contract.

b. EBRCSA Indemnification. EBRCSA will defend, indemnify, save, and hold harmless Contractor and its officers, agents and employees, if any, from any and all claims, demands, losses, costs, expenses, and liabilities for any damages, fines, sickness, death, or injury to person(s) or property, including any and all administrative fines, penalties or costs imposed as a result of an administrative or quasi-judicial proceeding, arising directly or indirectly from or connected with the services provided hereunder that are caused, or claimed or alleged to be caused, in whole or in part, by the negligence or willful misconduct of EBRCSA, its officers, employees, agents, contractors, subcontractors, or any persons under its direction or control. If requested by Contractor, EBRCSA will defend any such suits at its sole cost and expense. If Contractor elects to provide its own defense, EBRCSA will reimburse Contractor for any expenditures, including reasonable attorneys' fees and costs. EBRCSA is not required to indemnify Contractor for the proportion of liability a court determines is attributable to the negligence or willful misconduct of Contractor, its officers, agents and employees, if any. This provision will survive the expiration or termination of this Contract.

18. Insurance. During the entire term of this Contract and any extension or modification thereof, Contractor shall keep in effect insurance policies meeting the insurance requirements set forth in Exhibit A attached hereto and incorporated herein by reference.

19. Notices. All notices provided for by this Contract must be in writing and may be delivered by deposit in the United States mail, postage prepaid. Notices to Contractor must be addressed to the head of the county department for which this Contract is made. Notices to EBRCSA must be addressed to EBRCSA's address designated herein. The effective date of notice is the date of deposit in the mails

Initials: _____
EBRCSA County

or of other delivery, except that the effective date of notice to Contractor is the date of receipt by the head of the county department for which this Contract is made.

20. Nonrenewal. Contractor understands and agrees that there is no representation, implication, or understanding that the services provided by Contractor under this Contract will be purchased by EBRCSA under a new contract following expiration or termination of this Contract, and Contractor waives all rights or claims to notice or hearing respecting any failure to continue purchasing all or any such services from Contractor.

21. Possessory Interest. If this Contract results in Contractor having possession of, claim or right to the possession of land or improvements, but does not vest ownership of the land or improvements in the same person, or if this Contract results in the placement of taxable improvements on tax exempt land (Revenue & Taxation Code Section 107), such interest or improvements may represent a possessory interest subject to property tax, and Contractor may be subject to the payment of property taxes levied on such interest. Contractor agrees that this provision complies with the notice requirements of Revenue & Taxation Code Section 107.6, and waives all rights to further notice or to damages under that or any comparable statute.

22. No Third-Party Beneficiaries. Nothing in this Contract may be construed to create, and the parties do not intend to create, any rights in third parties.

23. Copyrights and Rights in Data. Contractor will not publish or transfer any materials produced or resulting from activities supported by this Contract without the express written consent of EBRCSA's Executive Director. If any material is subject to copyright, EBRCSA reserves the right to copyright, and Contractor agrees not to copyright such material. If the material is copyrighted, EBRCSA reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, and use such materials, in whole or in part, and to authorize others to do so.

24. Authorization. Contractor, or the representative(s) signing this Contract on behalf of Contractor, represents and warrants that it has full power and authority to enter into this Contract and to perform the obligations set forth herein.

25. No Implied Waiver. The waiver by EBRCSA of any breach of any term or provision of this Contract will not be deemed to be a waiver of such term or provision or of any subsequent breach of the same or any other term or provision contained herein."

Initials:

EBRCSA

County

EXHIBIT A

EBRCSA MINIMUM INSURANCE REQUIREMENTS

Without limiting any other obligation or liability under this Agreement, Contractor, at its sole cost and expense, shall secure and keep in force during the entire term of the Agreement or longer, as may be specified below, the following insurance coverage, limits and endorsements:

TYPE OF INSURANCE COVERAGES	MINIMUM LIMITS
A Commercial General Liability Premises Liability; Products and Completed Operations; Contractual Liability; Personal Injury and Advertising Liability	\$1,000,000 per occurrence (CSL) Bodily Injury and Property Damage
B Commercial or Business Automobile Liability All owned vehicles, hired or leased vehicles, non-owned, borrowed and permissive uses. Personal Automobile Liability is acceptable for individual contractors with no transportation or hauling related activities	\$1,000,000 per occurrence (CSL) Any Auto Bodily Injury and Property Damage
C Workers' Compensation (WC) and Employers Liability (EL) Required for all contractors with employees	WC: Statutory Limits EL: \$100,000 per accident for bodily injury or disease
D Endorsements and Conditions: <ol style="list-style-type: none"> 1. ADDITIONAL INSURED: All insurance required above with the exception of Personal Automobile Liability, Workers' Compensation and Employers Liability, shall be endorsed to name as additional insured: the EBRCSA, its members, officers, agents, employees and representatives, as their respective interests may appear but only with respect to derivative or imputed liability arising out of the Insured's performance of services under this Agreement for the EBRCSA. 2. DURATION OF COVERAGE: All required insurance shall be maintained during the entire term of the Agreement with the following exception: Insurance policies and coverage(s) written on a claims-made basis shall be maintained during the entire term of the Agreement and until three (3) years following termination and acceptance of all work provided under the Agreement, with the retroactive date of said insurance (as may be applicable) concurrent with the commencement of activities pursuant to this Agreement. 3. REDUCTION OR LIMIT OF OBLIGATION: All insurance policies shall be primary insurance to any insurance available to the Indemnified Parties and Additional Insured(s). Pursuant to the provisions of this Agreement, insurance effected or procured by Contractor shall not reduce or limit Contractor's contractual obligation to indemnify and defend the Indemnified Parties. 4. INSURER FINANCIAL RATING: Insurance shall be maintained through an insurer with a A.M. Best Rating of no less than A:VII or equivalent, shall be admitted to the State of California unless otherwise waived by Risk Management, and with deductible amounts acceptable to the EBRCSA. Acceptance of Contractor's insurance by the EBRCSA shall not relieve or decrease the liability of Contractor hereunder. Any deductible or self-insured-retention amount or other similar obligation under the policies shall be the sole responsibility of Contractor. 5. SUBCONTRACTORS: Contract shall include all subcontractors as an insured (covered party) under its policies and shall furnish separate certificates and endorsements for each subcontractor. All coverage for subcontractors shall be subject to all of the requirements stated herein. 6. JOINT VENTURES: If Contractor is an association, partnership or other joint business venture, required insurance shall be provided by any one of the following methods: <ul style="list-style-type: none"> - Separate insurance policies issued for each individual entity, with each entity included as a "Named Insured (covered party), or at minimum named as an "Additional Insured" on the other's policies. - Joint insurance program with the association, partnership or other joint business venture included as a "Named Insured. 7. CANCELLATION OF INSURANCE: All required insurance shall be endorsed to provide thirty (30) days advance written notice to the County of cancellation. 8. CERTIFICATE OF INSURANCE: Before commencing operations under this Agreement, Contractor shall provide Certificate(s) of Insurance and applicable insurance endorsements, in form and reasonably satisfactory to the EBRCSA, evidencing that all required insurance coverage is in effect. The EBRCSA reserves the rights to require Contractor to provide complete, certified copies of all required insurance policies. The require certificate(s) and endorsements must be sent to: <ul style="list-style-type: none"> - EBRCSA, Alameda County Office of Emergency Services, 4985 Broder Boulevard, Dublin, CA 94568, Attn: Executive Director. 	