



**STATE OF MICHIGAN
ENTERPRISE PROCUREMENT**

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **12**
to
Contract Number **MA190000001544**

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Various	Various
STATE	Contract Administrator	Nichole Harrell	DTMB
		517-449-9245	
		Harrelln@michigan.gov	

CONTRACT SUMMARY				
MPSCS Continued System Updates, Equipment, Maintenance and Upgrades, and Ancillary Systems Products				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE	
October 1, 2019	December 31, 2029	0 - 0 Months	December 31, 2029	
PAYMENT TERMS		DELIVERY TIMEFRAME		
Net 45		As per Delivery Order.		
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
<input checked="" type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS				
No Minimum Delivery Requirements.				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$211,232,622.44	\$0.00	\$211,232,622.44		

DESCRIPTION

Effective May 2, 2025, the parties agree to the following revisions to Section 1.3. Phase III - Cutover of the Schedule L, Statement of Work and corresponding pricing schedule. These products and services will be added utilizing existing funds for MSP use:

Work is divided into the following Sections and Costs/Credits:

1. MSP shall return the following equipment to Motorola Solutions resulting in a credit of \$83,526.18:
 - 04000-94331 Router ISR4331-SEC/K9 (qty 6) (\$7,723 ea) = \$46,338.00
 - 04000-14329 WARR 4331 SEC/K9 24X7 5YR (qty 6) (\$1,351/ea x 4yrs) = \$32,424.00
 - 809800-00199 Router CFG Fee (qty 6) (\$794.03/ea) = \$4,764.18
2. MSP is adding the following Equipment and Services:
 - Equipment costs totaling \$52,666.16:
 - 03800-07705 Router Nokia 7705 SAR-AX W/5YER SPT (Qty 4 \$12,174/ea) = \$48,696.00
 - 809800-00199 Router CFG Fee (qty 4) (\$794.03/ea) = \$3,176.12.00
 - 809800-00200 CFG Network Device (qty 4) (\$198.51/ea) = \$794.04
 - Managed Services costs totaling \$12,294.04:
 - 870891-66403 M&R Network/IP License (qty 4) (\$117.91/ea) = \$471.64
 - 809800-16347 M&R IP Device SRVC 5YR (qty 4) (\$2,955.60/ea) = \$11,822.40
 - VESTA Services costs totaling \$37,966.00:
 - 809800-17009 Field ENG Direct-Standard (qty 160) (\$112.50/ea) = \$18,000.00
 - 809800-51013 Project Management - Support (qty 2) (\$1,983/ea) = \$3,966.00
 - 809800-00128 NTWK INFRA Remote SCVS (qty 64) (\$250/ea) = \$16,000.00

Total Cost for Additional Equipment and Services = \$102,926.20

Applied Incentive = -\$25,731.55

Return Equipment Credit = -\$83,526.18

Total Cost Remaining = Credit (\$6,331.53)

All other terms, conditions, specifications and pricing remain the same. Per Vendor and agency agreement and DTMB Central Procurement Services approval.

**Program Managers
for
Multi-Agency and Statewide Contracts**

AGENCY	NAME	PHONE	EMAIL
DTMB	Kate Jannereth	517-881-1031	jannerethk@Michigan.gov
MSP	Jonathon Whitford	517-512-4068	WhitfordJ@michigan.gov
MSP	Andrew Richards	517-242-2560	RichardsA4@michigan.gov



**STATE OF MICHIGAN
ENTERPRISE PROCUREMENT**

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **11**
to
Contract Number **MA190000001544**

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Various	Various
STATE	Contract Administrator	Nichole Harrell	DTMB
		517-449-9245	
		harrelln@michigan.gov	

CONTRACT SUMMARY				
MPSCS Continued System Updates, Equipment, Maintenance and Upgrades, and Ancillary Systems Products				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE	
October 1, 2019	December 31, 2029	0 - 0 Months	December 31, 2029	
PAYMENT TERMS		DELIVERY TIMEFRAME		
Net 45		As per Delivery Order.		
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
<input checked="" type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS				
No Minimum Delivery Requirements.				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$211,232,622.44	\$0.00	\$211,232,622.44		

DESCRIPTION

Effective December 26, 2024, the parties agree to add Schedule A - Attachment 12 - Statement of Work for ASTRO and PremierOne Managed Detection & Response, Schedule B.3. - Pricing, Schedule R -Professional Services Addendum, and Schedule S - Data Processing Addendum as attached, which detail products and services necessary for the protection of the Michigan public safety network. These products and services will be added utilizing existing funds for MPSCS use.

Work is divided into the following Sections and costs:

Operational Costs

1. ASTRO Managed Detection and Response w/ATI: \$1,564,115.80
2. PremierOne MDR: \$36,687.04
3. ASTRO Support Services, Dispatch & Onsite Support: \$282,494.74

System Integration Costs

1. System Integration, Hardware, EDR Licensing & Training: \$1,122,861.35
2. Juniper Intrusion Detection Credit: \$120,000.00

Professional Services

1. NIST 800-53r5 SSP: \$340,720.00

Total Project Cost: \$3,226,878.93

All other terms, conditions, specifications and pricing remain the same. Per Contractor and agency agreement and DTMB Central Procurement Services approval.

**Program Managers
for
Multi-Agency and Statewide Contracts**

AGENCY	NAME	PHONE	EMAIL
MSP	Andrew Richards	517-242-2560	RichardsA4@michigan.gov
MSP	Jonathon Whitford	517-512-4068	WhitfordJ@michigan.gov
DTMB	Kate Jannereth	517-881-1031	jannerethk@Michigan.gov

SCHEDULE A – ATTACHMENT 12 - STATEMENT OF WORK

Contract No. 190000000154

ASTRO and PremierOne Managed Detection & Response and Professional Services

BACKGROUND

The Michigan Public Safety Communications System (MPSCS) was established to provide a unified, Statewide radio communications system which may be utilized by all emergency entities that wish to use it statewide. This Contract covers all of the Statements of Work for the MPSCS in relation to the ASTRO 25 public safety communications network. This includes annual maintenance and support contract as well as new technology.

SCOPE

Under Change Notice No. 11 the MPSCS will be implementing Motorola Solutions proposed infrastructure security Managed Detection Response (MDR) solution and professional services, which will provide the ASTRO P25 public safety communications network with 24/7 monitoring against threat and intrusion.

This Statement of Work Includes:

1. Service Onboarding
2. Infrastructure Readiness
3. System Buildout and Deployment
4. Monitoring “Turn Up”
5. Service Commencement

PROJECT OBJECTIVE

The Contractor must provide the following MDR and risk mitigation services as specified in Schedule B.3., Pricing Additions:

- ASTRO MDR
- PremierOne MDR
- Professional Services
- On-Site Dispatch

1. Solution Description – ASTRO MDR

1.1. Solution Overview

Motorola will provide access to our ActiveEye 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 MDR features and services are included:

1. ActiveEye Managed Detection and Response Elements
 - a. ActiveEye Security Management Platform
 - b. ActiveEye Remote Security Sensor (AERSS)
2. Service Modules
 - a. Log Collection / Analytics
 - b. Network Detection
 - c. External Vulnerability Scanning
 - d. Endpoint Detection and Response
 - e. Advanced Threat Insights
3. 24/7 Monitoring and Support

1.2. Service Description

Managed Detection and Response is performed by Motorola using the ActiveEye security platform. The security 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.

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

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

1.2.1. Managed Detection and Response Elements

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

1.2.1.1. ActiveEye Security Platform

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

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

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

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

1.2.1.2. ActiveEye Managed Security Portal

The ActiveEye Managed Security Portal will synchronize security efforts between the Customer and Motorola. 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.

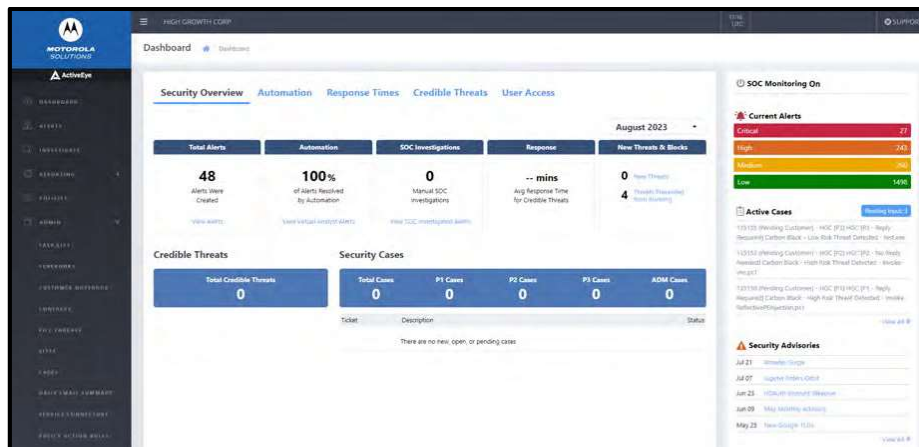


Figure 1-1: ActiveEye Portal

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 identify a threat, the analysts will create a security case. Through the ActiveEye Portal, the Customer can view details of current or past 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 ActiveEye 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:

1. Bulletins - Instructions from the Customer, or the security team, that 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.

2. Customer Notebook - The security team will use the Customer Notebook to document the Customer’s environment and any specific network implementation details that will help the security team investigate security cases.
3. 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 security team 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.

1.2.1.3. 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 ActiveEyeS 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 5-15 P
Heat Dissipation (max)	2107 BTU/hr.
Internet Service Bandwidth	Bandwidth throughout 10Mbps per zone

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

1.2.1.4. Internetworking Firewall

Motorola introduces a formalized and centralized Internet connection to the ASTRO® 25 system using an Internetworking Firewall. The Internetworking Firewall serves as a security barrier and demarcation point between a master site and the Internet (or a customer network leading to the Internet). The Internetworking Firewall supports traffic for various ASTRO® 25 features that require access to the Internet. The Internetworking Firewall sits between the Demilitarized Zone (DMZ) and the Internet (or customer network leading to the Internet).

The following are the environmental requirements and specifications the Customer must provide to prepare for the Internetworking Firewall deployment, if one is required.

Specifications	Requirements
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

1.2.2. 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 Customer’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.

1.2.2.1. Log Collection / Analytics

The AERSS deployed in the system collects logs and other security information from applicable servers, workstations, switches, routers, 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 security team 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 1-3: Service Modules for subscription details.

1.2.2.2. 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 security team for further analysis.

1.2.2.3. External Vulnerability Scanning

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

1.2.2.4. Endpoint Detection and Response

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

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

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

1.2.3. Motorola ASTRO Security Team

Motorola delivers Monitoring using one or more geographical locations. Those locations include any centralized hardware and software used to deliver this Service and its service modules. The security team and its centralized hardware and software are housed within an SSAE-18 compliant data center.

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

1.2.4. Advanced Threat Insights

With Advanced Threat Insights (ATI), Motorola provides continuous dark web monitoring, alerts and notifications, customer risk reviews, organization-specific threat intelligence, and industry-level threat intelligence. Trained security analysts will search the dark web looking for indications that any of the Customer's systems, customer user accounts in the monitored domain, or data sets have been compromised. In addition, security analysts will search for evidence that the Customer's organization or primary applications may be the target of a threat actor campaign.

Motorola's security analysts will develop threat reports and review them with the Customer. Analysts perform threat intelligence gathering using a combination of automated and human methods. They review threat intelligence findings during normal US business hours 8x5 on standard US business days: Monday through Friday 8AM to 5PM local time, excluding US Holidays.

Dedicated Security Experts

Motorola maintains highly trained security experts skilled in monitoring the dark web and surface web that will perform threat intelligence gathering on your behalf, alerting you to threats and indications of compromise. With Advanced Threat Insights, you will have a named security analyst to provide consistent knowledge and to be available for questions during regular business hours, 9AM-5PM ET.

Customer Risk Review

Make staying informed on threats to your organization easier with monthly customer risk reviews. Motorola security experts will walk the Customer through threat intelligence findings and provide other information that may contextualize the threats the Customer faces.

Focused Agency Threat Intelligence Report

Reporting to key stakeholders in your organization is easy with a prepared customer threat intelligence report tailored to your organization.

Public Safety Industry Threat Report

Stay current with threats that are facing the Public Safety industry at large with the Motorola Public Safety Industry Threat Report.

Service Dependencies

Motorola's Advanced Threat Insights is a premium level of the service coordinated with standard operations for our Managed Detection and Response (MDR) customers. As such, ATI must be purchased in combination with MDR Services for ASTRO systems.

2. ASTRO MDR

2.1. Overview

Motorola's ASTRO® 25 MDR provides monitoring of radio network security information by specialized security analysts with extensive experience working with ASTRO® 25 mission-critical networks.

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

2.2. Description of Service

2.2.1. Deployment Timeline and Milestones

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

Phase 1: Service Onboarding

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

The Customer will be provisioned onto the ActiveEye MDR portal and be able to configure key contacts for interaction with the infrastructure security team. The portal will enable service notifications, access to vulnerability scans and security advisories. The first external vulnerability scan will be conducted and reported when approved by MPSCS. The Customer will receive instructions for accessing the Incident Response (IR) teams within the first 30 days. Once access is provisioned, the customer will receive any assistance required from the IR team.

Phase 2: Infrastructure Readiness

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

Phase 3: System Buildout and Deployment

Motorola 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 may be required to deploy software and/or configurations in cases where Motorola Solutions does not manage the device and does not have access or authorization to perform the installation.

Motorola Solutions will coordinate with the customer to identify and schedule mutually agreeable maintenance windows where Motorola Solutions will perform integration of endpoint detection and response agents at in-scope sites and Customer Enterprise Networks (CENs). Integration of endpoint detection and response agents within the zone core and dispatch sites will be scheduled in conjunction with an ASTRO 25 system upgrade.

Phase 4: Monitoring "Turn Up"

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

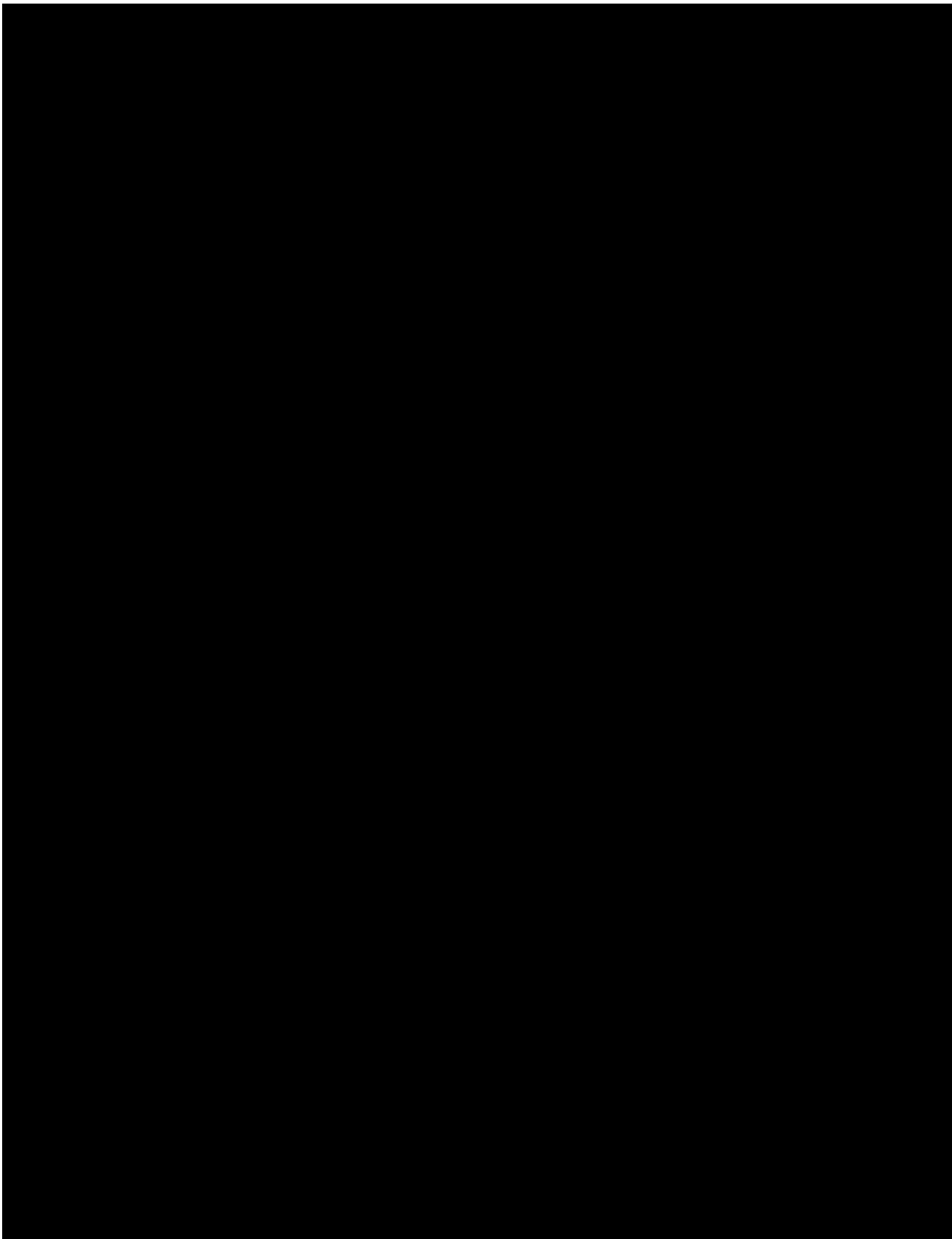
Phase 5: Tuning/Report Setup

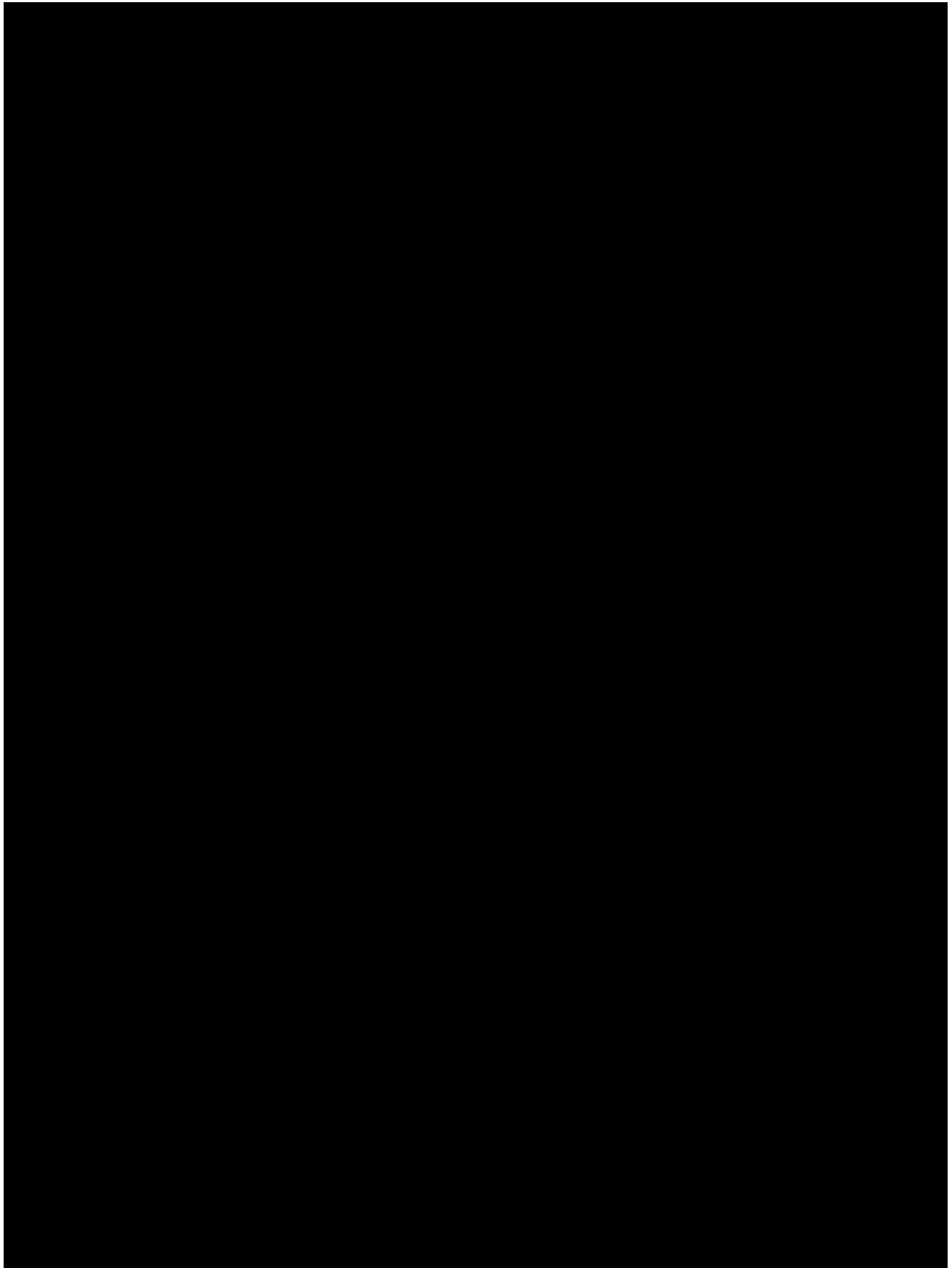
Motorola will conduct initial tuning of the events and alarms in the service and conduct an additional ActiveEye Portal training session.

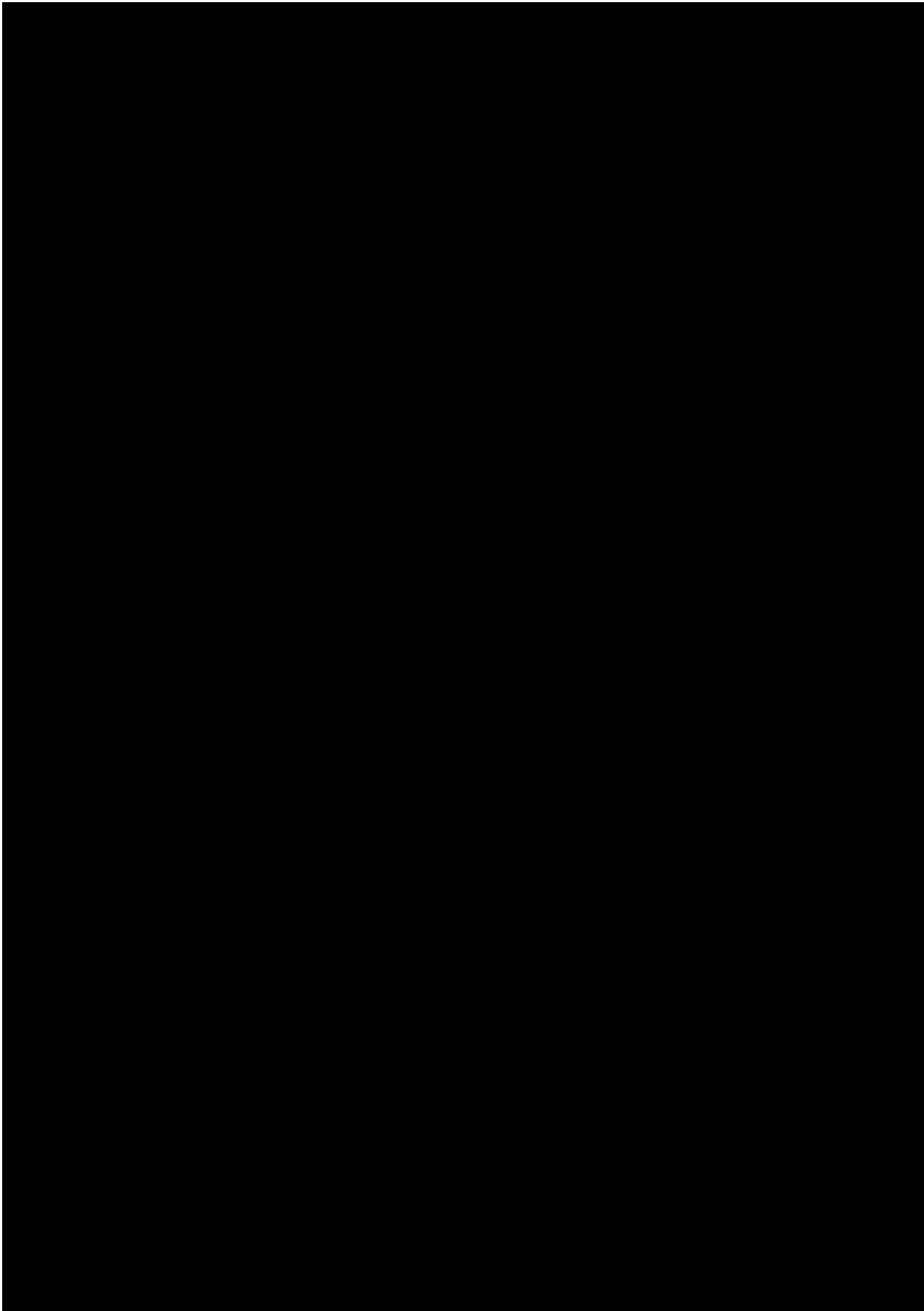
Service Commencement

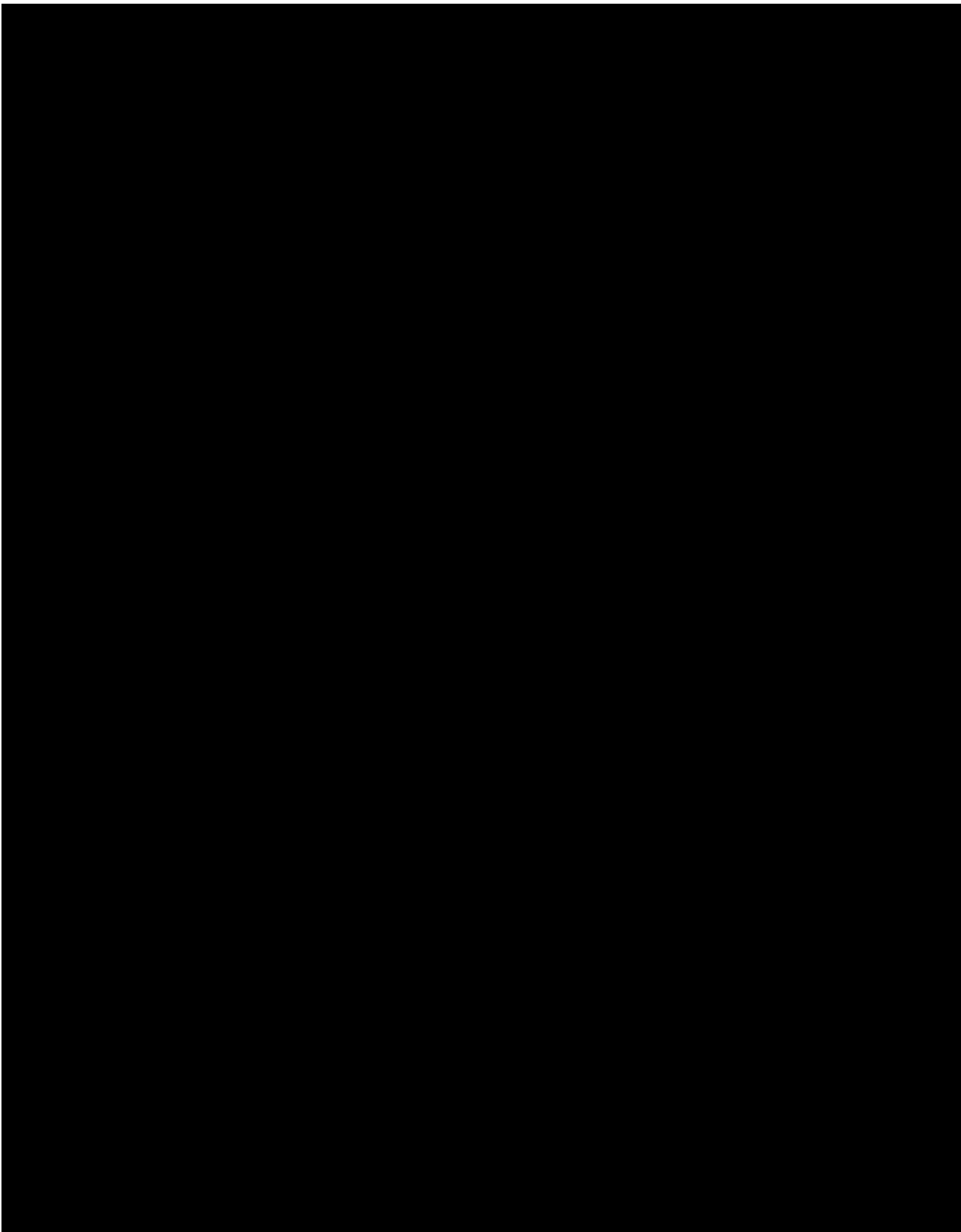
The Service will commence after provisional ATO has been approved by the DTMB and beneficial use has been established.

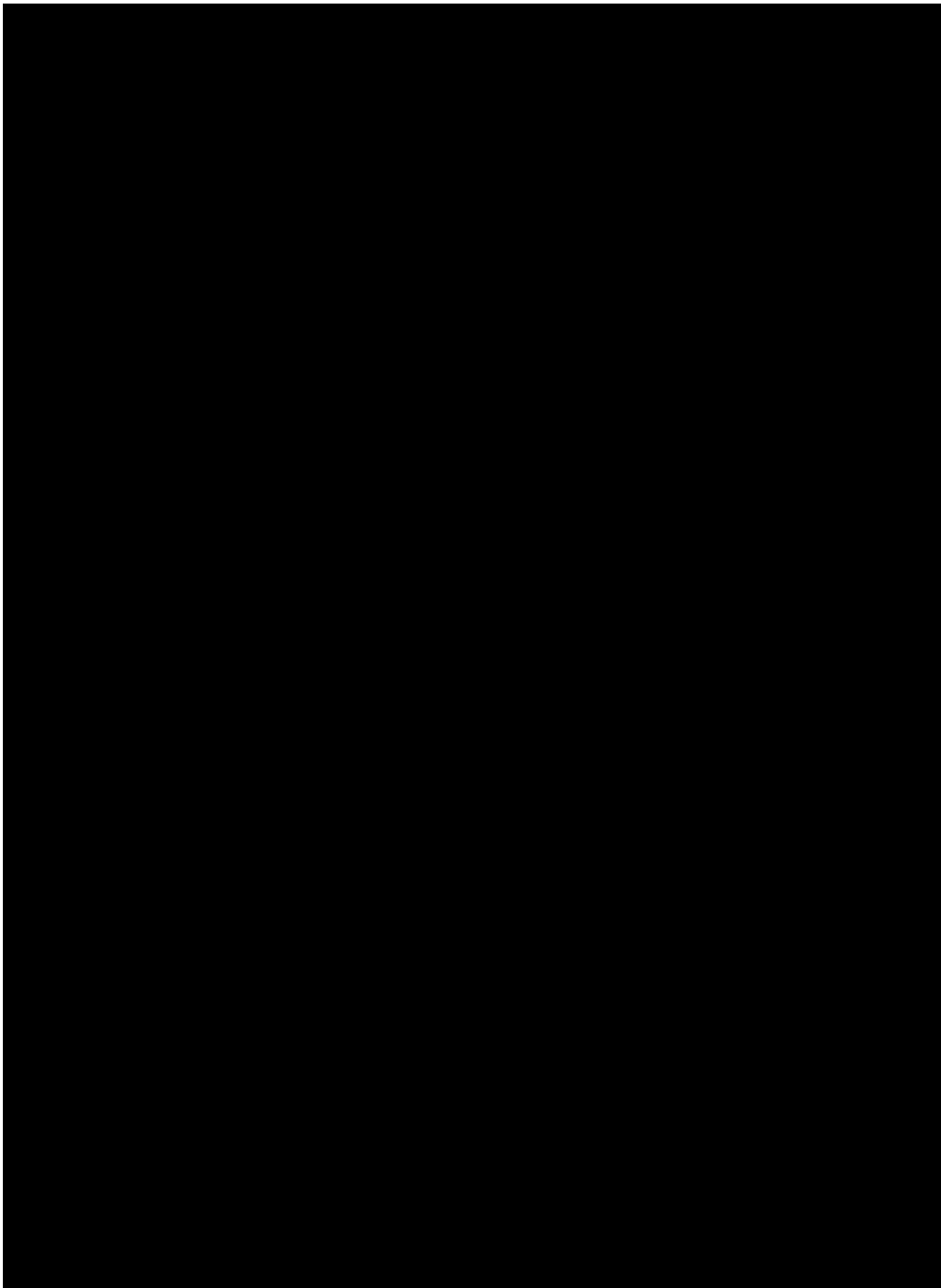
In the case of a new ASTRO system, the Service will commence in parallel to the commencement date of the core ASTRO Service package "Turn Up" date. Motorola and the Customer will collaborate to complete the additional deployment tasks.

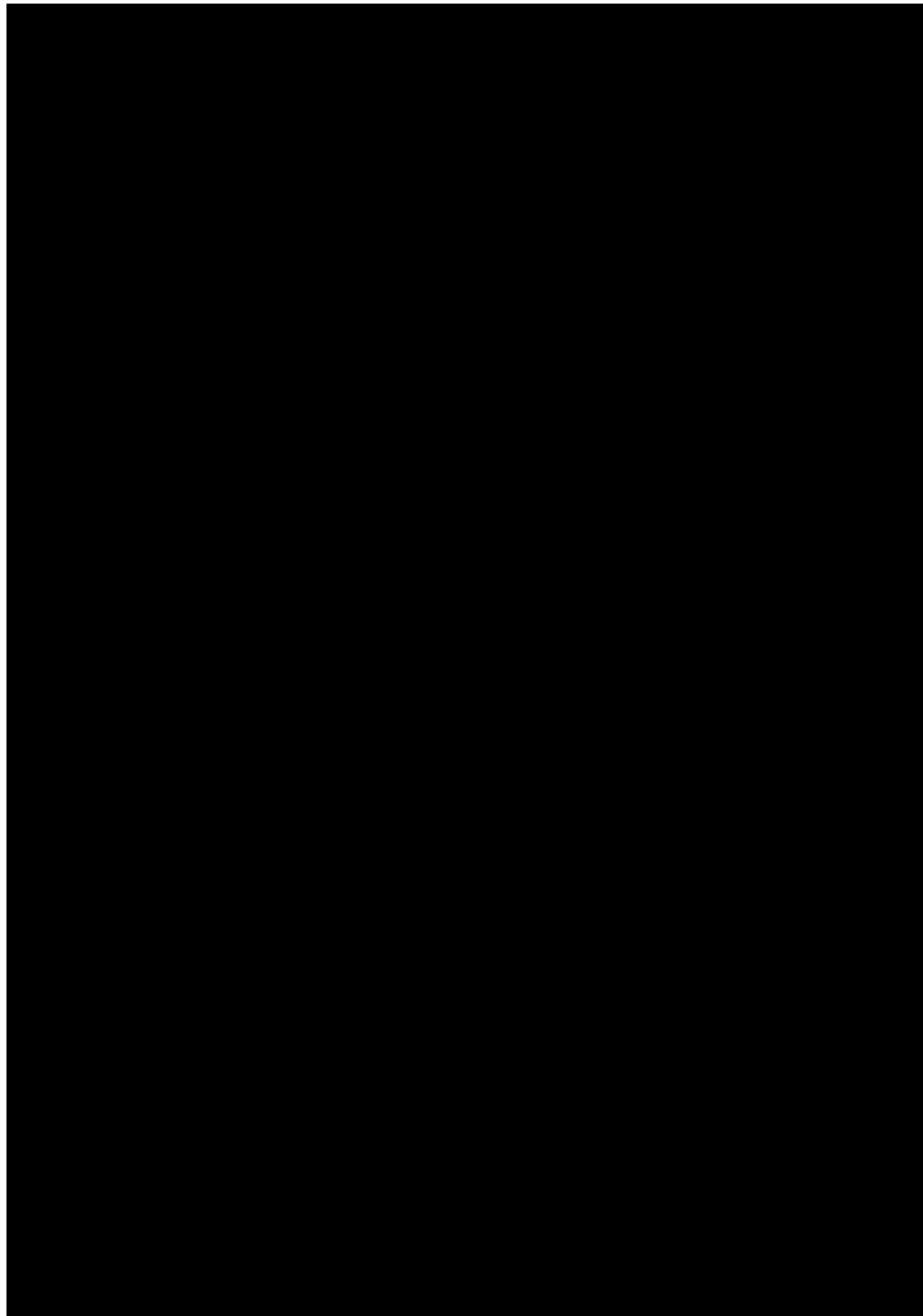


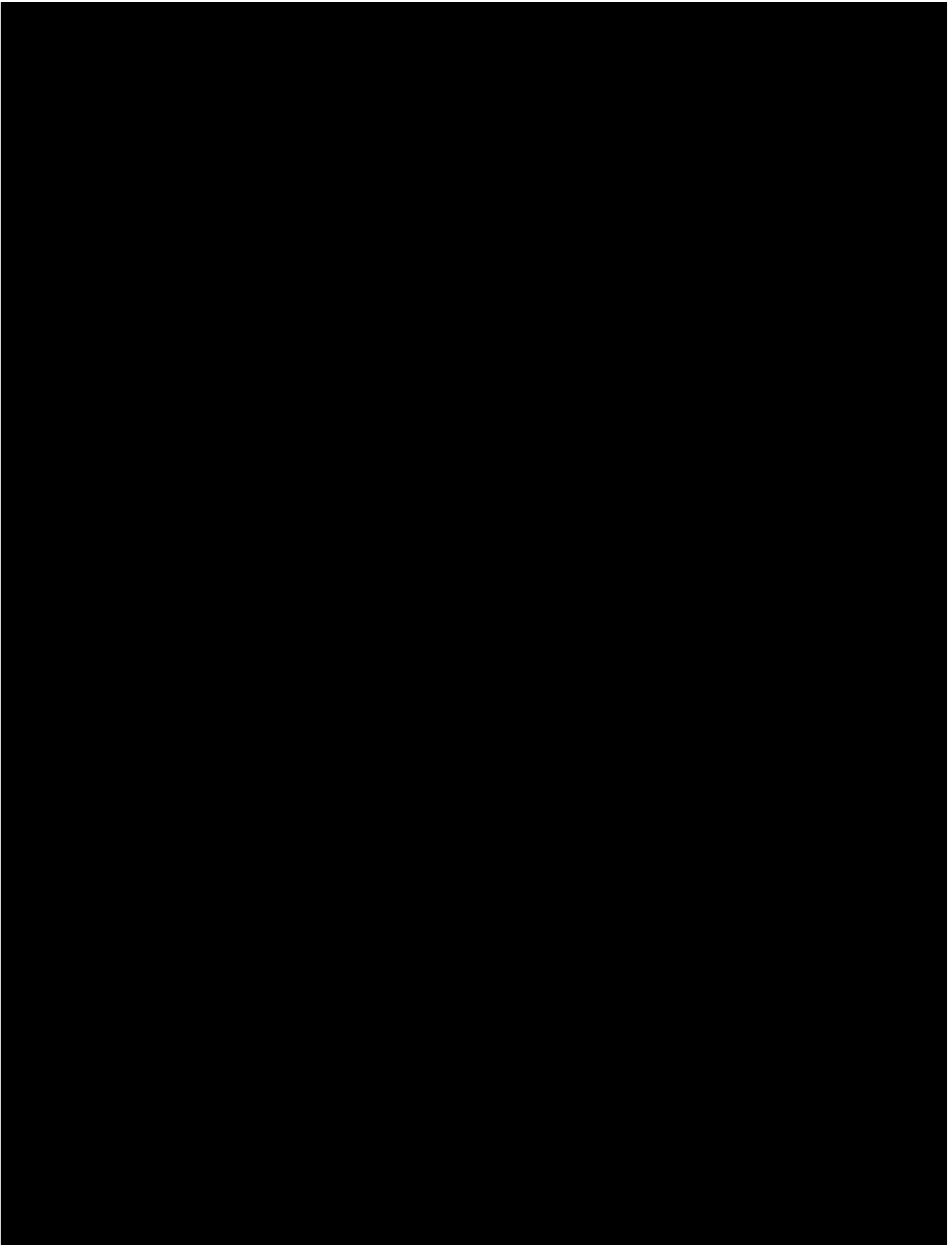


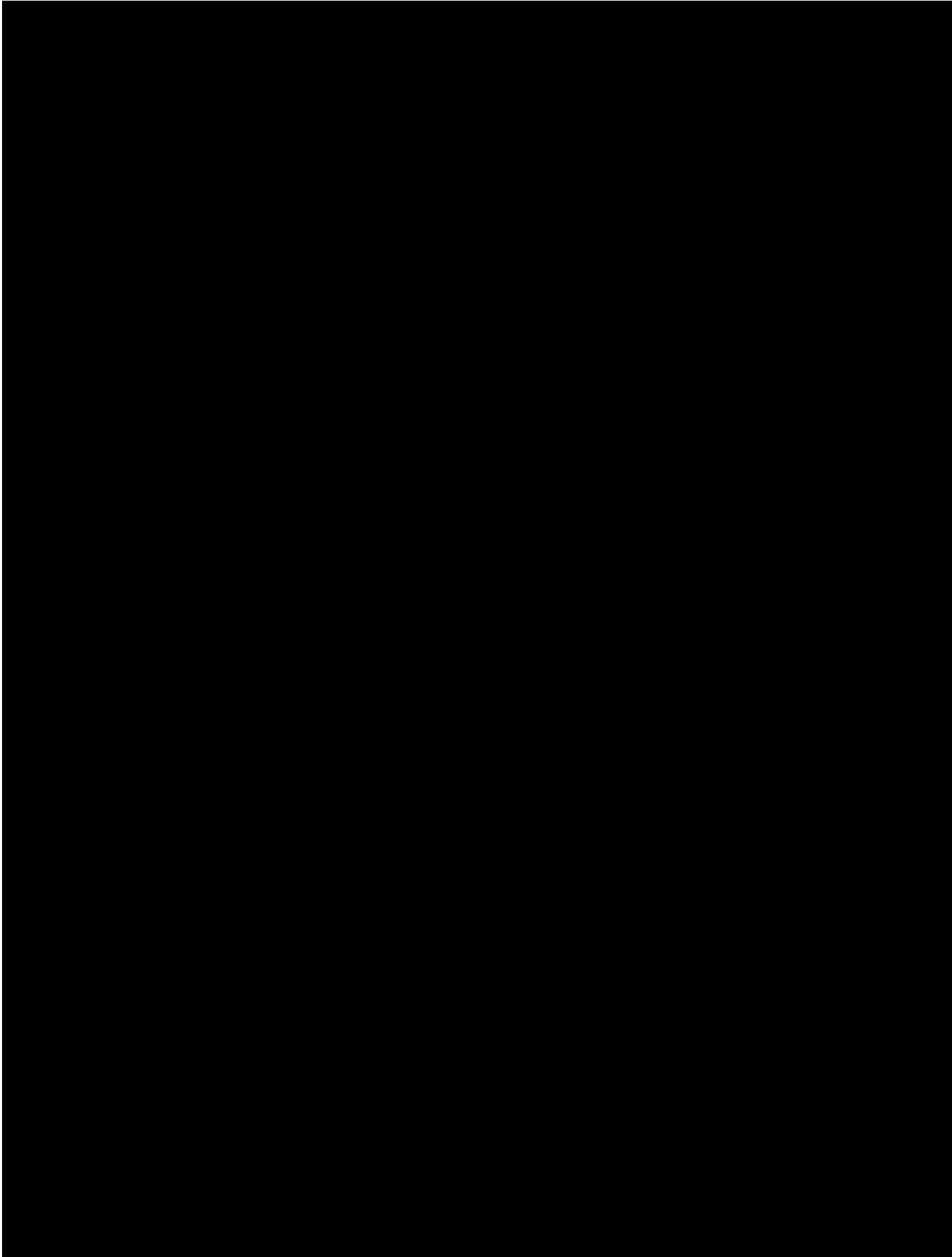


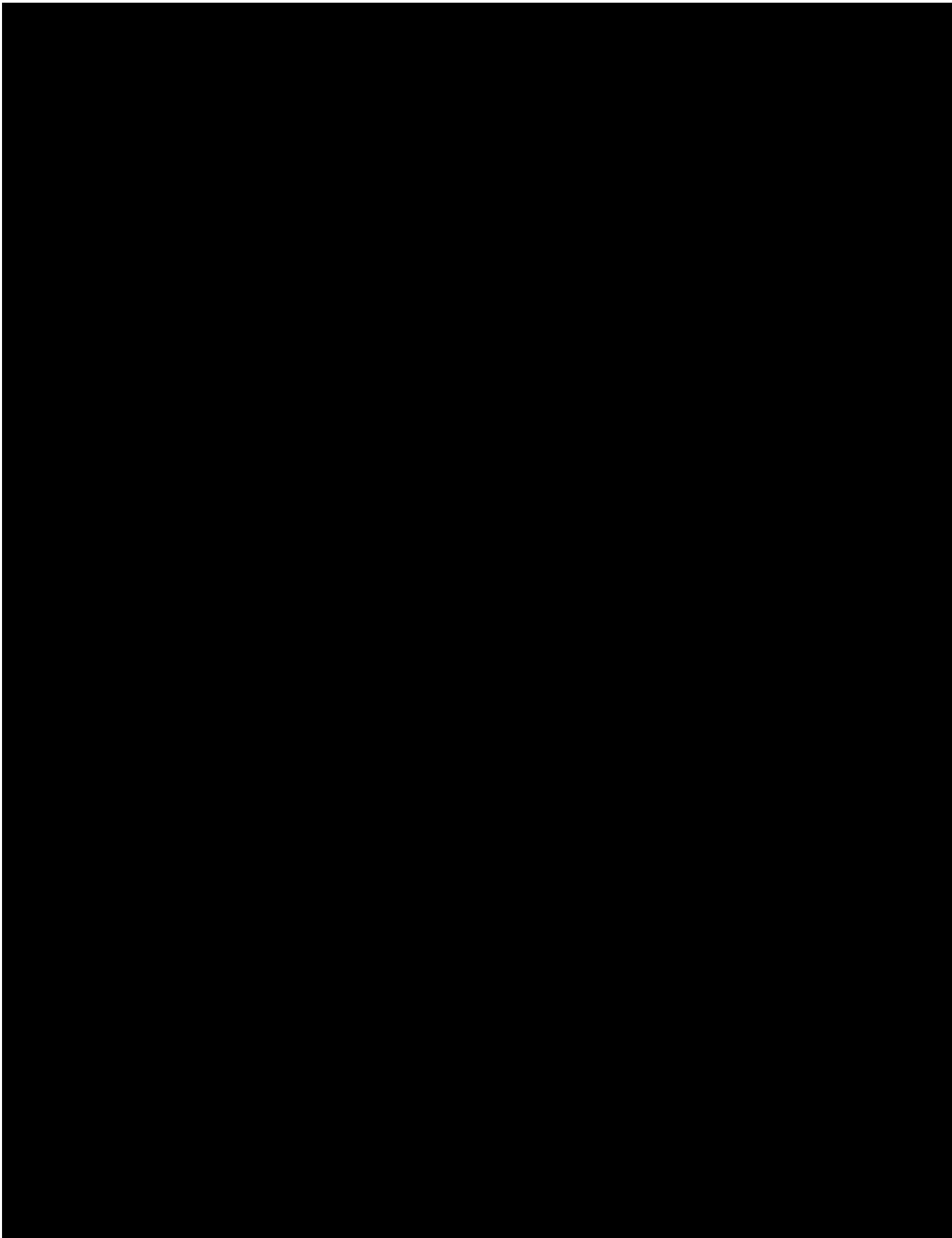












2.2.5. General Requirements

Motorola Responsibilities

1. 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.
 - a. If the Centralized Event Logging feature is not installed on the Customer's ASTRO 25 RNI, Motorola will install it as part of this service.
2. Coordinate with the Customer on any system changes necessary to integrate the AERSS into the system and establish necessary connectivity.
3. Provide software and licenses to the Customer necessary to remotely monitor the ASTRO 25 network and applicable CEN environments.
4. Verify connectivity and monitoring is active prior to start of service.
5. Coordinate with the Customer to maintain Motorola service authentication credentials.
6. Monitor the Customer's ASTRO 25 network and applicable CEN systems 24/7/365 for malicious or unusual activity.
7. Integrate EDR agents as per the "Deployment Timeline and Milestones" section in all network segments where endpoint detection and response is in scope.
 - a. Note that network segments with insufficient connectivity to support endpoint detection and response will be considered out of scope for endpoint detection and response. See Customer Responsibilities section 2.2.5.2 for bandwidth requirements.
 - b. Motorola will perform the installation of endpoint detection and response agents in the RNI-DMZ CEN(s) for all Motorola managed devices that support endpoint detection and response agents.
 - c. Motorola will support the customer with installing endpoint detection and response agents in the RNI-DMZ CEN(s) for any device that supports endpoint detection and response agents and is not Motorola Solutions managed.
8. Respond to security incidents in the Customer's system in accordance with Section 2.3.6: Incident Priority Level Definitions and Response Times. This may include, but is not limited to, requesting additional information from the Customer, continuing to monitor the event for further development or informing the Customer to enact the Customer's documented Incident Response plan.
9. Assist the Customer with identifying devices that support logging within the ASTRO 25 network and that applicable CEN systems have been configured to forward Syslog events to the AERSS.
10. Assist the Customer with the installation of log forwarding agents on systems that are not managed by Motorola. Note, Motorola will perform installation on all endpoints that are managed by Motorola.

11. Provide the Customer with access to the ActiveEye platform enabling Customer access to security event and incident details.
12. Remove McAfee Anti-virus on all endpoints where Endpoint detection and response (EDR) is installed
13. Install Endpoint detection and response (EDR) agents on all identified endpoints in the system during a scheduled ASTRO upgrade phase.
14. Decommission Central Security Management Server once all endpoints have been migrated from McAfee anti-virus to EDR.
15. Motorola will install EDR for re-imaged or re-installed endpoints during upgrade phases until the end of the service agreement.
16. Motorola will update TNCT to accommodate Endpoint Detection and Response where necessary. This includes firewall changes, ASTRO link modifications, and endpoint configuration changes. Backhaul configuration changes are excluded.

MPSCS Responsibilities

1. The ASTRO25 MDR service requires a connection from the Customer's ASTRO 25 network and applicable CEN systems to the Internet. Establish connectivity with sufficient bandwidth before service commences. Internet service bandwidth requirements are as follows:
 - a. Bandwidth throughput of 10MB per zone core location.
 - b. Bandwidth at least 2Mbps per dispatch site location.
 - c. High availability Internet Connection (99.99% (4-9s) or higher)
 - d. Packet loss < 0.5%
 - e. Jitter < 10 ms
 - f. Delay < 120 ms
 - g. RJ45 Port Speed - Auto Negotiate
2. Maintain an active subscription for:
 - a. Security Update Service (SUS) (or Remote Security Update Service), ensuring patches and antivirus definitions are applied according to the release cadence of the service.
 - b. ASTRO Dispatch Service and ASTRO Infrastructure Response.
3. 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). It is the Customer's responsibility or the contracted maintainer to install the AERSS device in the Control Room CEN.
4. Allow Motorola continuous remote access to monitor the ASTRO 25 network and applicable CEN systems. This includes keeping the connection active, providing passwords, and working with Motorola to understand and maintain administration privileges.

5. Provide continuous utility service(s) to any equipment installed or utilized at the Customer's premises to support service delivery and remote monitoring.
6. Provide Motorola with contact information necessary to complete the Customer Support Plan (CSP). Notify the Customer's Customer Support Manager (CSM) within two weeks of any contact information changes.
7. Notify Motorola if any components are added to or removed from the environment as it may be necessary to update or incorporate in Managed Detection and Response. Changes to monitored components may result in changes to the pricing of the Managed Detection and Response service.
8. As necessary, upgrade the ASTRO 25 system, on-site systems, and third-party software or tools to supported releases.
9. Allow Motorola's dispatched field service technicians physical access to monitoring hardware when required.
10. Cooperate with Motorola and perform all acts that are required to enable Motorola to provide the services described in this SOW.
11. 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.
12. Respond to security Incident Cases created by Motorola.

2.2.6. Service Modules

The following subsections describe the delivery of the service modules selected in Table 1-3: Service Modules.

2.2.6.1. Log 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 security team for further analysis.

Motorola Responsibilities

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

MPSCS Responsibilities

1. If applicable, configure customer-managed networking infrastructure to allow AERSS to Communicate with ActiveEye as defined.

2. If applicable, configure any Customer managed devices in the CEN to forward data to ActiveEye.

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

2.2.6.2. Network Detection

The AERSS deploys a Network Intrusion Detection System (NIDS), 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 security team for further analysis.

Motorola Responsibilities

1. Work with the Customer to integrate AERSS.
2. Optimize the policies and configuration to tune out noise and highlight potential threats.
3. The security team consults with the Customer to identify the appropriate deployment of Network Detection Service Components. The security team will 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.

MPSCS Responsibilities

1. If necessary, configure Customer's networking infrastructure to allow AERSS to communicate with ActiveEye as defined.
2. 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.
3. Initiate recommended response actions when active attacks are detected.

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

2.2.6.3. External Vulnerability Scanning

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

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

Motorola Responsibilities

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

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

MPSCS Responsibilities

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

Applies to internet facing assets only.

2.2.6.4. Advanced Threat Insights

With Advanced Threat Insights, Motorola provides continuous dark web monitoring, alerts and notifications, customer risk reviews, organization-specific threat intelligence and industry-level threat intelligence. Trained security analysts will search the dark web looking for indications that any of the Customer's systems, customer user accounts in the monitored domain, or data sets have been compromised. In addition, security analysts will search for evidence that the Customer's organization or primary applications may be the target of a threat actor campaign.

Motorola's security analysts will develop threat reports and review them with the Customer. Analysts perform threat intelligence gathering using a combination of automated and human methods. They review threat intelligence findings during normal US business hours 8x5 on standard U.S. business days: Monday through Friday 8 a.m. to 5 p.m. local time, excluding U.S. holidays.

There are four main aspects of this service:

- 1. Named Analyst** – A dedicated analyst will work with the Customer to understand the organization's operating environment and architecture in more detail and depth. This approach enables the analyst to provide detailed recommendations for improving the Customer's overall risk posture from a consistent single point of contact.
- 2. Proactive Threat Hunting** – The analyst will dedicate time each month (number of hours dependent on subscription) to evaluate available threat intelligence and sensor information (log analysis, EDR, NIDs, etc.) to identify areas of concern. This manual investigation can uncover previously undetected threats that exist outside of the scope of typical security alerting and provide a starting point for remediation and security recommendations to improve the Customer's overall security posture. The focus of this work can be directed by

the customer toward the most critical assets or those assets most at risk given the threat landscape at the time.

- 3. Surface, Deep, and Dark Web Insights** – Risks go beyond the visible boundaries of the organization. Monitoring for key assets on the surface, deep, and dark web provides actionable insights into how the organization is being targeted and what assets are at risk, such as lost or exposed credentials and sensitive data.
- 4. Monthly Summary and Discussion of Findings** - The assigned analyst will present key findings for the past month, discuss new threats to consider, and suggest any additional security measures relevant to the Customer’s organization.

Motorola Responsibilities

1. Coordinate with the Customer to collect relevant information necessary to complete threat intelligence searches on the dark web.
2. Deliver a monthly risk report detailing threat intelligence specific to the Customer.
3. Provide the Customer with a monthly public safety industry intelligence report detailing threat intelligence related to the public safety community as a whole.
4. Hold recurring formal risk reviews with the Customer to evaluate threats facing the Customer and intelligence discoveries. This review also serves as an opportunity to refine the list of critical information the threat team needs to proactively search for.
5. Alert the Customer immediately when critical threats or information breaches are discovered.

MPSCS Responsibilities

1. Coordinate with Motorola to maintain relevant information necessary to complete threat intelligence searches on the dark web.
2. Obtain for Motorola all rights, if any, which may be necessary to permit requested threat intelligence searches on the dark web.

Disclaimer

Scope of services do not include employee related investigative services, such as those that may target any specific employees (or other individuals) or implicate privacy rights, alleged or suspected internal conduct, or rights that may be protected or regulated by law, e.g. information bearing on an individual’s character, general reputation, personal characteristics, mode of living, etc. Motorola reserves the right to withhold from Customer any information deemed outside the scope of the engagement or otherwise subject to legal restrictions and take any other action it deems to be required by law.

Customer understands that some information shared with Customer through the Advanced Threat Insights service will, by its nature, be unverifiable, will be delivered on an as-is basis, and may or may not be correct. Customer agrees any information shared is for Customer’s governmental purpose use only and shall not be further distributed by Customer.

Motorola does not represent that it will identify, fully recognize, discover, or resolve all security events or threats, system vulnerabilities, malicious codes or data, backdoors, or other system threats or incompatibilities as part of the service, or that the agreed upon cadence/time of delivery will be sufficient to identify, mitigate or prevent any cyber incident.

For subscribers of the Advanced Threat Insights service, Motorola disclaims any warranty and does not guarantee to be able to locate all threat intelligence on the surface, deep or dark web. Motorola will perform an expansive search but cannot cover every forum and information source.

2.2.6.5. Endpoint Detection and Response

Endpoint detection and response agents deployed on in-scope and supported Windows and Linux hosts and servers throughout the system constantly monitor for indicators of compromise and feed this information back to the ActiveEye Security Platform. The infrastructure security team monitors this feed and is ready 24x7 to take action when a detection is made.

Motorola Responsibilities

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

MPSCS Responsibilities

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

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

2.3. Monitoring and Support

2.3.1. Scope

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

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

Motorola will start monitoring the ASTRO® 25 MDR service in accordance with Motorola processes and procedures after deployment, as described in Section 2.2.1: Deployment Timeline and Milestones.

The security team 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 security team will respond to detected events in accordance with Section 2.3.6: Incident Priority Level Definitions and Response Times.

2.3.2. Ongoing Infrastructure Security Team Service Responsibilities

Motorola Responsibilities

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

1. Engage the Customer's defined Incident Response Process.
2. 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.
3. Analysis and support to help the Customer determine if the Customer's corrective actions are effective.
4. Continuous monitoring, in parallel with analysis, to support incident response.

MPSCS Responsibilities

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

2.3.3. 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 24 hours a day, 7 days a week.

Motorola Responsibilities

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

MPSCS Responsibilities

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

Limitations and Exclusions

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

2.3.4. Incident Response

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

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

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

Motorola Responsibilities

1. Upon the identification of an IoC, notify the Customer's documented contact and initiate the escalation plan.
2. Take documented, Customer approved actions in an attempt to contain an IoC to the extent enabled via Motorola managed technology. Communicate to the Customer any additional potential containment actions and incident response resources that can be taken across the Customer's managed IT infrastructure.
3. 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.
4. Document and share IoC and artifacts discovered during investigation. Motorola services exclude performing on-site data collection or official forensic capture activities on physical devices.

MPSCS Responsibilities

1. Maintain one named PoC to coordinate regular team discussions and organize data collection and capture across the Customer and Motorola teams.
2. 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.

2.3.5. Event Response and Notification

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

Table 2-1: 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 security team analysis. Notification procedures are included in Table 2-2: Notification Procedures.

Notification

Table 2-2 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 will notify the Customer according to the escalation and contact procedures defined by the Customer and Motorola during the implementation process.

Tuning

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

Motorola will provide the Customer with the ability to temporarily suppress alerts reaching ActiveEye, enabling a co-managed approach to tuning and suppressing events or alarms. The

security team 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 may make recommendations to the Customer to adjust the configurations of their installed software so Services can be effectively delivered. Service Availability will not be applicable during the tuning period and responses or notifications may not be delivered. However, Motorola will provide responses and notifications during this period.

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

2.3.6. Incident Priority Level Definitions and Response Times

Priority for an alert-generated incident or EOI is determined by the ActiveEye Platform analytics that process multiple incoming alert feeds, automation playbooks, and security analyst knowledge.

Incident Priority	Incident Definition	Notification Time
Critical P1	<p>Security incidents that have caused or are suspected to have caused significant 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/EDR. • Evidence that a monitored component has communicated with suspected malicious actors. 	Response provided 24 hours, 7 days a week, including US public holidays.
High P2	<p>Security incidents that have localized impact and may become more serious if not quickly addressed. Effort to recover from the incident may be moderate to significant.</p> <p>Examples:</p> <ul style="list-style-type: none"> • Malware that is quarantined by antivirus/EDR. • Multiple behaviors observed in the system that are consistent with known attacker techniques. • Suspected unauthorized attempts to log into user accounts. 	Response provided 24 hours, 7 days a week, including US public holidays.

Incident Priority	Incident Definition	Notification Time
	<ul style="list-style-type: none"> • Suspected unauthorized changes to system configurations, such as firewalls or user accounts. 	
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 include:</p> <ul style="list-style-type: none"> • Observed failures of security components. • Informational events. • User account creation or deletion. • Privilege change for existing accounts. 	<p>Response provided on standard business days, Monday through Friday 8:00 a.m. to 5:00 p.m. CST/CDT, excluding US public holidays.</p>
Low P4	<p>These are typically service requests from the Customer.</p>	<p>Response provided on standard business days, Monday through Friday from 8:00 a.m. to 5:00 p.m. CST/CDT, excluding US public holidays.</p>

2.3.6.1. Response Time Goals

Priority	Response Time
Critical P1	<p>An security team Security Analyst will make contact with the customer technical representative within one (1) hour of the request for support being logged in the issue management system or the creation of an alert suggesting an infrastructure security incident that requires action. Continual effort will be maintained to identify the extent of the incident and provide actions for containment.</p>
High P2	<p>An security team Security Analyst will make contact with the customer technical representative within four (4) hours of the request for support being logged at the issue management system or the creation of an alert suggesting an infrastructure security incident that requires action. Continual effort will be maintained to identify the extent of the incident and provide actions for containment.</p>
Medium P3	<p>An security team Security Support Engineer will make contact with the customer technical representative within the next business day of the request for support being logged at the issue management system or the</p>

Priority	Response Time
	creation of an alert suggesting an infrastructure security incident that requires action.
Low P4	An security team Security Support Engineer will make contact with the Customer technical representative within seven business days of the logged request for support at the issue management system.

2.3.6.2. ActiveEye Platform Availability

The platform utilizes a multi-zone architecture which can recover from failures in different data collection, enhancement, analysis, and visualization tiers. Motorola will make commercially reasonable efforts to provide monthly availability of 99.9% for the ActiveEye Platform services. Service availability is subject to limited scheduled downtime for servicing and upgrades, as well as unscheduled and unanticipated downtime resulting from circumstances or events outside of Motorola’s reasonable control, such as disruptions of, or damage, to the Customer’s or a third-party’s information or communications systems or equipment, telecommunication circuit availability/performance between Customer sites, any on-premises core and/or between on-premises equipment and the ActiveEye Platform.

2.3.6.3. ActiveEye Remote Security Sensor

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

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

2.3.7. ASTRO MDR Training

The following training will be available or will be made available to MPSCS.

Training	Details	Expected Time
ActiveEye 101	Basic training to familiarize MPSCS with the ActiveEye Portal and use case in the network environment.	1 Hour
Self-Guided ActiveEye Training Videos	Motorola is in the process of developing self-guided videos to navigate the ActiveEye platform. These videos will be shared when available.	Self-Guided
Learning Portal	Materials on ActiveEye, EDR, MDR, and ASTRO systems are posted and will continue to be posted	Self-Guided

Training	Details	Expected Time
	to the subscribed learning portal for MPSCS to access.	
Advanced Threat Intelligence Dedicated Analyst	MPSCS will receive a dedicated analyst that can be reached from 9-5 CST to assist with questions/concerns on the ActiveEye platform.	Varies

3. Solution Description – PremierOne MDR

3.1. Solution Overview

The following infrastructure security services are included in the PremierOne system Statement of Work:

1. ActiveEye Managed Detection & Response for PremierOne
 - a. Endpoint Detection and Response
2. Motorola Infrastructure Security Services

3.2. Services Included

The ActiveEye service modules included in this schedule are included below:

Table 3-1. Service Modules

Service Module	Features Included	Site/Environment
Endpoint Detection and Response (EDR)	<ul style="list-style-type: none"> • Palo Alto Cortex • (100) EDR Total Endpoints • Online Storage Period: 30 Day Storage 	PremierOne Host Environment (100)
Infrastructure Security Team	<ul style="list-style-type: none"> • Monitoring and Support 	Service Modules

4. PremierOne MDR

4.1. Project Deployment

In order to establish initial expectations for deployment, Motorola will work with Customer to help you understand the impact of introducing a new solution and your preparedness for the implementation and support of PremierOne Managed Detection and Response.

Motorola Responsibilities

1. Motorola will schedule a service kick-off meeting with the Customer and provide information-gathering documents to the customer within 30 days of contract signature. The kick-off meeting will be conducted remotely at the earliest mutually available opportunity.
2. Motorola will provide detailed requirements regarding Customer infrastructure preparation actions within one week of the kick-off meeting.

3. Motorola will provision tools in accordance with the requirements of this Service, and consistent with information gathered in earlier phases. Motorola will also provide detailed, required Customer deployment actions within one-week of the completion of all infrastructure readiness tasks.

MPSCS Responsibilities

1. The Customer must attend the kick-off meeting and complete information gathering documents as quickly and accurately as possible.
2. The Customer must accomplish all infrastructure preparation tasks as quickly as possible.

4.2. ActiveEye Platform

Motorola will provide 24/7 access to the ActiveEye platform. Motorola will notify Customer if access will be affected by scheduled maintenance.

Motorola Responsibilities

1. Provide access to the ActiveEye portal for Customer and any identified, approved users. After initial deployment, Customer will have self-service access to add/remove/update user access as needed.
2. Provide the services subscribed to, as noted in Table 3-1. Service Modules.
3. Make monthly services implementation and status reports available to Customer.
4. Resolve platform issues and technical errors as documented by Customer.
5. Retain security logs within ActiveEye. Security logs will be retained for the length of time designated by the short-term storage policy selected by Customer.

MPSCS Responsibilities

1. Provide reasonable assistance to Motorola to perform the Service, as described in this SOW. This assistance includes, but is not limited to, technical assistance with issues that may require physical access to the devices affected by this Service, or virtual assistance with virtual environment issues that require administrative access to devices affected by this Service.
2. Provide all technical, license, and service information requested in the implementation documents prior to the commencement of the Service.
3. Perform all network and system integrations necessary for ActiveEye Service. This includes providing external connectivity for ActiveEye security components.
4. Ensure network bandwidth of up to 10 Mbps per host environment.
5. Install agents on in-scope systems and devices, as required.
6. Configure all necessary components of Customer's infrastructure to integrate with ActiveEye.
7. Provide the name, email, landline telephone numbers, and mobile telephone number for all shipping, installation, and security Points of Contact (POC)s.

4.2.1. Endpoint Detection and Response

Motorola Responsibilities

1. Provide ports and protocols to the Customer for the EDR solution.
2. Deploy and maintain EDR agents to PremierOne host environment.
3. Configure EDR solution to enable ActiveEye connection for event/alert collection and response actions.

MPSCS Responsibilities

1. Deploy and maintain EDR agents to required customer-owned client workstations and handheld devices, as applicable. (CAD Mobile Clients)
2. Configure networking infrastructure to allow EDR agents to communicate with centralized server components.
3. Comply/consent with the terms of applicable licenses, privacy statements, or other third-party agreements to the extent third-party software or services are utilized or provided by/through Motorola Solutions, including applicable EDR solution provider's end user license agreements ("EULAs"), if any.
4. Obtain any third-party consent required to enable Motorola to provide the monitoring service, if applicable.

4.2.2. 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 24 hours a day, 7 days a week.

Motorola Responsibilities

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

MPSCS Responsibilities

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

Limitations and Exclusions

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

4.3. Infrastructure Security Monitoring and Support

Motorola's Infrastructure Security team will provide continuous 24x7 monitoring through automated tools and review by trained security analysts. Motorola will analyze events and notify Customer in accordance with Table 4-2. Notification Procedures.

Motorola will start monitoring the Service in accordance with Motorola processes and procedures after deployment, as described in Section 4.1 Project Deployment.

Customer will be able to open a support request for the security team via a toll-free telephone number or email address, available 24/7. Support requests are stored in a ticketing system for accountability and reporting.

4.3.1. Ongoing Service Responsibilities

Motorola Responsibilities

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

1. Engage Customer's defined Incident Response Process
2. Attempt to determine the root cause and extent of compromise using existing monitoring capabilities in place as part of the Service.
3. Analysis and support to help Customer determine if Customer's corrective actions are effective.
4. Continuous monitoring, in parallel with analysis, to support incident response.

MPSCS Responsibilities

1. Provide Motorola with accurate and up-to-date information, including the name, email, landline telephone numbers, and mobile telephone numbers for all designated, authorized Customer escalation Points of Contact (POC).
2. Provide a Network Map detailing Customer's network architecture for network(s) in scope for the Service, if available.
3. Provide a timely response to security team security incident tickets or investigation questions.
4. Provide an established service window in which qualified IT personnel will be able to respond to major event escalations.
5. Notify Motorola at least twenty-four (24) hours in advance of any scheduled maintenance, network administration activity, or system administration activity that would affect Motorola's ability to perform the Managed Service, as described in this SOW.

4.3.2. Service Module Specific Services

With this service, Motorola's security team will provide specific services for ActiveEye platform service modules Customer is subscribed to. In addition, security team services can be augmented by Advanced Threat Insights.

The following describes these modules.

4.3.2.1. Managed Endpoint Detection and Response

Motorola's security team will consult with Customer on the deployment of the Endpoint Detection and Response (EDR) solution. The security team will advise, on an ongoing basis, what security policies should be updated to optimize threat detection.

The security team will consult with Customer to define a response automation plan that outlines the scenarios where the security team should take automatic response actions on systems within Customer environment. In cases outside the automatic response scenarios, the security team will open Security Cases with Customer with recommended actions and await approval before taking actions.

The security team will track suspicious files and processes in Customer environment to report threat trends on what new threats are being discovered vs. previously seen threats.

Motorola Responsibilities

1. Provide recommendations on endpoint security policy and configuration to optimize threat identification.
2. Maintain, with input from Customer, an automatic response plan for defined endpoint security scenarios or malware types.

MPSCS Responsibilities

1. Initiate response actions on endpoint solutions when not defined as automatic actions or not available as remote actions on the EDR solution in use.

4.3.3. Event Response, Notification, and Tuning

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

Incident Priority	Incident Navigation	Response Time
Critical P1	<p>Security incidents that have caused or are suspected to have caused significant and/or widespread damage to the functionality of the Customer’s PremierOne 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. 	Response provided 24 hours, 7 days a week, including US Public Holidays.
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>	Response provided 24 hours, 7 days a week, including US Public Holidays.

Incident Priority	Incident Navigation	Response Time
	<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. • Suspected unauthorized attempts to log into user accounts. • Suspected unauthorized changes to system configurations, such as firewalls or user accounts. 	
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 include:</p> <ul style="list-style-type: none"> • Observed failures of security components. • Informational events. • User account creation or deletion. • Privilege change for existing accounts. 	Response provided from 8:00a.m. to 5:00p.m. CST/CDT, Monday through Friday, excluding U.S. Public Holidays.
Low P4	These are typically service requests from the Customer.	Response provided from 8:00a.m. to 5:00p.m. CST/CDT, Monday through Friday, excluding U.S. Public Holidays.

4.3.3.1. Notification

Contractor will establish notification procedures with agency, generally categorized in accordance with the following table.

Table 4-2. 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.

Notification Procedure	Details
Urgent Notification Procedure	Additional, optional means and addresses for notifications of Events of Interest that require urgent notification. These usually include telephone notifications.

Contractor will notify agency according to the escalation and contact procedures defined by agency and Contractor during the implementation process.

4.3.3.2. Tuning

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

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

4.3.3.3. Tuning Period Exception

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

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

Motorola Responsibilities

1. Motorola will monitor the service and check in-scope assets are properly forwarding logs or events and that system scans are functioning. Motorola will notify the customer of any exceptions. Motorola will begin monitoring any properly connected, in-scope sources after the tuning period.
2. Motorola will conduct initial tuning of the events and alarms in the service, as well as set up initial reports (User Access, Administration Events, and Configuration Findings Reports).

MPSCS Responsibilities

1. Customer must provide appropriate connectivity for all in-scope assets to the service and address any exceptions noted by Motorola. Failure to do so will delay completion of future phases and will prevent Motorola from monitoring those sources.

2. Customer must deploy tools, as applicable, in their environment, in accordance with provided requirements. Customer must engage the security team in discussing the tuning approach and confirm the configurations requested.

4.3.4. Limitations and Exclusions

This Service excludes any incident response support actions outside those outlined within this SOW, such as those that require Motorola personnel to directly access Customer devices, travel, deploy new tools, or direct specific actions. These services may be obtained from Motorola through a separate proposal.

4.3.5. PremierOne MDR Training

The following training will be available or will be made available to MPSCS.

Training	Details	Expected Time
ActiveEye 101	Basic training to familiarize MPSCS with the ActiveEye Portal and use case in the network environment.	1 Hour
Self-Guided ActiveEye Training Video	Motorola is in the process of developing self-guided videos to navigate the ActiveEye platform. These videos will be shared when available.	Self-Guided
Learning Portal	Materials on ActiveEye, EDR, MDR, and ASTRO systems are posted and will continue to be posted to the subscribed learning portal for MPSCS to access.	Self-Guided

5. Solution Description – Professional Services

The following infrastructure security services are included in this statement of work:

- System Security Plan Development

5.1. Site Information

The following site information is included in this statement of work:

Table 5-1: Customer Site Information

Quantity	Site / Location	Network Environment	Service Type
1	Organization Level	ASTRO RNI Only	System Security Plan Development

Backhaul environments are not included.

Table 5-2: Services by Year

Year	Service	Description
1	System Security Plan Development	Infrastructure Security Incident Management Plan Review and Development

5.2. Service Description

5.2.1. System Security Plan Development – NIST 800-53r5

A System Security Plan (SSP) is a formal document that provides a comprehensive and detailed overview of the security requirements for an information system, or for an information security program. The SSP describes the security controls in place, or those planned for meeting the requirements outlined in a security framework such as NIST 800-53r5.

The Motorola team is comprised of accredited individuals with years of experience in the public and private sectors implementing, auditing, and certifying systems in a variety of contexts and risk levels.

6. Professional Services

6.1. System Security Plan and Security Accreditation Process.

Security Accreditation Process. Throughout the Term, Contractor will assist the State, with its **Security Accreditation Process**, which includes the development, completion and on-going maintenance of a system security plan for the MPSCS (SSP) using the State’s automated governance, risk and compliance (GRC) platform, which requires Contractor to submit evidence, upon request from the State, in order to validate Contractor’s security controls within thirty (30) days of the State’s request. On an annual basis, or as otherwise required by the State such as for significant changes, re-assessment of the system’s controls will be required to receive and maintain authority to operate (ATO). All identified risks from the SSP will be remediated through a Plan of Action and Milestones (POAM) process with remediation time frames and required evidence based on the risk level of the identified risk. For all findings associated with the Contractor’s solution, Contractor will be required to participate in negotiations around the creation of State approved POAMs, perform related remediation activities within mutually agreeable timeframes if not otherwise dictated by applicable standards or FBI CJIS Policy, and provide evidence of compliance. For clarity, the State makes all decisions on the level of risk it is willing to accept.

7. On-Site Support Dispatch

7.1. Overview

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.

7.2. Description of Service

The Motorola Solutions CMSO Service Desk will receive the Customer or Motorola’s security team 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 7.9 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.

7.3. Scope

On-site Infrastructure Response is available in accordance with Section 7.9 Priority Level Definitions and Response Times. Customer's Response Time Classification is designated in the Customer Support Plan.

7.4. Geographic Availability

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

7.5. Inclusions

On-site Infrastructure Response is provided for Motorola Solutions-provided infrastructure that exists at the primary zone cores. The list includes:

1. Core Server Architecture
2. ActiveEye Remote Security Sensors
3. Network Management Clients
4. Motorola Provided RNI-DMZ CEN Devices
5. Co-located Dispatch Consoles & Archiving Interfacing Servers
6. Motorola Provided Routing Equipment
7. Motorola Provided Switching Equipment
8. Motorola Provided Firewalls

7.6. Limitations and Exclusions

The following items are excluded from this service:

1. All Motorola Solutions infrastructure components beyond the post-cancellation support period.
2. All third-party infrastructure components beyond the post-cancellation support period.
3. All broadband infrastructure components beyond the post-cancellation support period.
4. Physically damaged infrastructure components.
5. Third-party equipment not shipped by Motorola Solutions.

6. Consumable items including, but not limited to, batteries, connectors, cables, toner or ink cartridges, tower lighting, laptop computers, monitors, keyboards, and mouse.
7. Video retrieval from digital in-car video equipment.
8. 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.
9. Racks, furniture, and cabinets.
10. Tower and tower mounted equipment.
11. Non-standard configurations, customer-modified infrastructure, and certain third party infrastructure.
12. Firmware or software upgrades.

7.7. Motorola Solutions Responsibilities

1. Receive service requests.
2. 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.
3. Dispatch a field service technician, as required by Motorola Solutions' standard procedures, and provide necessary incident information.
4. Provide the required personnel access to relevant Customer information, as needed.
5. Motorola Solutions field service technician will perform the following on-site:
6. Run diagnostics on the infrastructure component.
7. Replace defective infrastructure components, as supplied by the Customer.
8. Provide materials, tools, documentation, physical planning manuals, diagnostic and test equipment, and any other material required to perform the maintenance service.
9. If a third-party vendor is needed to restore the system, the vendor can be accompanied onto the Customer's premises.
10. 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.
 - a. Escalate the incident to the appropriate party upon expiration of a response time.
11. Close the incident upon receiving notification from the Customer or Motorola Solutions field service technician, indicating the incident is resolved.
12. Notify the Customer of incident status, as defined in the CSP and Service Configuration Portal ("SCP"):

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

7.8. MPSCS Responsibilities

1. Contact Motorola Solutions, as necessary, to request service.
2. Prior to start date, provide Motorola Solutions with the following pre-defined Customer information and preferences necessary to complete CSP:
 - a. Incident notification preferences and procedure.
 - b. Repair verification preference and procedure.
 - c. Database and escalation procedure forms.
3. Submit timely changes in any information supplied in the CSP to the Customer Support Manager (“CSM”).
4. Provide the following information when initiating a service request:
 - a. Assigned system ID number.
 - b. Problem description and site location.
 - c. Other pertinent information requested by Motorola Solutions to open an incident.
5. Provide field service technician with access to equipment.
6. Supply infrastructure spare or FRU, as applicable, in order for Motorola Solutions to restore the system.
7. Maintain and store software needed to restore the system in an easily accessible location.
8. Maintain and store proper system backups in an easily accessible location.
9. 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.
10. Cooperate with Motorola Solutions and perform reasonable or necessary acts to enable Motorola Solutions to provide these services.
11. 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.

7.9. Priority Level Definitions and Response Times

Incident Priority	Incident Navigation	Response Time
Critical P1	<p>Core: Core server or core link failure. No redundant server or link available.</p> <p>Security Features: Security is non-functional or degraded.</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>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>Field service technician arrival on-site within 4 hours of receiving dispatch notification.</p>
Medium P3	<p>Consoles: Up to 20% of a site's console positions down.</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>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>Not applicable.</p>

8. Limitations and Clarifications

8.1. Limitations and Exclusions

Motorola's ASTRO MDR service 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 completion of a Customer's Incident Response Plan.

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

8.1.1. Service Limitations

Security services are inherently limited and will not guarantee that the Customer's system will be error-free or immune to security breaches as a result of any or all of the services described in this SOW. Motorola does not warrant or guarantee that this service will identify all security 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.

8.1.2. Customer and Third-Party Information

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

8.2. Applicable Third-Party Software End User Terms

Additional license terms apply to third-party software included in certain software Products, see Exhibit 1 to this Schedule A, Attachment 12 – Third Party License Terms and Conditions. Customer will comply, and ensure its Authorized Users comply, with all such additional license terms. If the modified license terms are determined to be materially detrimental to Customer, in the Customer's sole discretion, then Customer may terminate the Services.

9. Pricing Summary

9.1. Operational / Annual Costs

Operational Costs	
Term	10/1/2024 – 9/30/2025
ASTRO Managed Detection and Response w/ ATI	\$1,564,115.80
PremierOne MDR. Includes 100 EDR Licenses	\$36,687.04
ASTRO Support Services, Dispatch & Onsite Support	\$282,494.74

Year 1 Total	
MPSCS Total	\$1,883,297.58

9.2. Operations / Annual Costs Payment Terms

Period of Performance

The initial MDR subscription period of the contract will extend until September 30, 2025, 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.

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 will invoice the Customer for all service fees in advance for the Operational Costs prorated amount based on the commencement date of service according to the Pricing table in Section 9.1.1.

Customer will make payments to Motorola within forty-five (45) 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.

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.

9.3. Capital Costs (One-Time)

One-Time Capital Costs	
System Integration, Hardware, EDR Licensing & Training	\$1,122,861.35
Juniper Intrusion Detection Credit	\$120,000.00
One-Time Capital Costs Total	\$1,002,861.35

9.4. Capital Costs Payment Terms

Payment Milestones – System Integration, PM, Hardware, & Training		
Milestone	Percentage	Terms
Contract Execution	25%	Due upon Effective Date
Shipment	60%	Motorola Solutions shall make partial shipments of equipment and will request payment upon shipment of such equipment.
System Integration	10%	Motorola Solutions shall invoice for installations completed on a site-by-site, section by section basis.

Payment Milestones – System Integration, PM, Hardware, & Training		
System Acceptance	5%	The value of the equipment shipped/services performed will be determined by the value of shipped services as a percentage of the total milestone value.

The value of the equipment shipped/services performed will be determined by the value shipped/services performed as a percentage of the total milestone value. Unless otherwise specified, contract discounts are based upon all items proposed and overall system package. For invoicing purposes only, discounts will be applied proportionately to the FNE and Subscriber equipment values to total contract price. Overdue invoices will bear simple interest at the maximum allowable rate by state law.

9.5. Professional Services (One-Time)

Professional Services	
NIST 800-53r5 SSP	\$340,720.00

9.6. Professional Services Payment Terms

Except for a payment that is due on the Effective Date, Customer will make payments to Motorola Solutions within forty-five (45) days after the date of each invoice. Customer will make payments when due in the form of a check, cashier’s check, or wire transfer drawn on a U.S. financial institution. Payment for the System purchase will be in accordance with the following milestones:

Payment Milestones – System Integration, PM, Hardware, & Training		
Milestone	Percentage	Terms
Contract Execution	75%	Due upon Effective Date
80% SSP Controls Complete	15%	Motorola Solutions shall invoice when professional services milestones are met.
SSP Completion and Full Authority to Operate (ATO)	10%	Motorola Solutions shall invoice when professional services are completed.

**Exhibit 1 to Schedule A, Attachment 12
Third Party License Terms and Conditions**

**Palo Alto EULA
(see following pages)**



END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT (“Agreement”) GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS (as that term “Product” is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS “CUSTOMER”, “END USER”, “YOU” or “YOUR”) AND (A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55, LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS “PALO ALTO NETWORKS”).

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose (“Evaluations”), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

“**Affiliate**” means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where “Control” means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise. Customer acknowledges and authorizes Palo Alto Networks’ use of all Palo Alto Networks Affiliates to deliver Products and Services.

“**End User Data**” means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

“**Enterprise Program**” means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

“**Hardware**” means hardware-based products listed on Palo Alto Networks’ then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

“**Product**” means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

“**Published Specifications**” mean the applicable user manual, the WildFire Acceptable Use Policy found at <https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy>, the applicable Service Level Agreement found at <https://www.paloaltonetworks.com/services/support/support-policies.html>, and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product.

“**Software**” means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

“Subscription(s)” means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

“Systems Data” means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

- i. in accordance with Published Specifications for the Product;
- ii. solely within the scope of the use rights purchased (e.g., number of users);
- iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and
- iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

- i. in accordance with Published Specifications for the Product;
- ii. solely within the usage capacity purchased (e.g., number of workloads);
- iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and
- iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions

You shall not:

- i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;
- ii. use the Products beyond the scope of the use right and/or capacity purchased;
- iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;
- iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;
- v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;
- vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;
- vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;
- viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be subject to the [Palo Alto Networks license transfer procedure \(https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html\)](https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);
- ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;
- x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival

or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section 5.b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer's access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network's discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks' Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

- i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;
- ii. Software shall substantially conform to Palo Alto Networks' Published Specifications for three (3) months from the date of fulfillment; and
- iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repair or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

- i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;
- ii. accident, negligence, abuse or misuse of a Product;
- iii. use of the Product other than in accordance with Published Specifications;
- iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or
- v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED "AS IS". PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks' suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks' suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

- i. death or bodily injury;
- ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and
- iii. Customer's payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party's patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a "**Claim**"), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

- i. procure the right for you to continue using the Product;
- ii. replace or modify the Product to avoid the Claim; or
- iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

- i. modifications to a Product made by a party other than Palo Alto Networks or its designee;
- ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;
- iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;
- iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or
- v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"**Confidential Information**" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party ("**Discloser**"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by

the party receiving such information (“**Recipient**”). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

- i. was in the public domain at the time it was communicated to Recipient;
- ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;
- iii. was in Recipient’s possession free of any obligation of confidentiality at the time it was communicated to Recipient;
- iv. was disclosed to Recipient free of any obligation of confidentiality; or
- v. was developed by Recipient without use of or reference to Discloser’s Confidential Information.

Each party will not use the other party’s Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser’s Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser’s Confidential Information:

- a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;
- b. on a confidential basis to its legal or professional financial advisors; or
- c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the [Data Processing Addendum](#), which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the

time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at <https://www.paloaltonetworks.com/support/support-policies/grace-period.html>

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

- i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.
- ii. for Palo Alto Networks: legal@paloaltonetworks.com; or,
- iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("**Open-Source Software**"). A list of Open-Source Software can be found at <https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html>. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "**QATT**") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications solely to identify Customer as a Palo Alto Networks customer. Other than as expressly stated herein, neither party shall use the other party's name, logo or trademarks without the prior written permission of the other party.

n. Survival

Sections regarding license restrictions, ownership, term and termination, U.S. Government End Users, limitations of liability, governing law, and this General section shall survive termination of this Agreement.

o. Waiver and Severability

The failure by either party to enforce any provision of this Agreement will not constitute a waiver of future enforcement of that or any other provision. Any waiver or amendment of any provision of this Agreement will be effective only if in writing and signed by authorized representatives of both parties. If any provision of this Agreement is held to be unenforceable or invalid, that provision will be enforced to the maximum extent possible and the other provisions will remain in full force and effect.

p. U.S. Government End Users

This section applies to United States Government end users only and does not apply to any other end users. The Software and its documentation are "commercial computer software" and "commercial computer software documentation," respectively; as such terms are used in FAR 12.212 and DFARS 227.7202. If the Software and its documentation are being acquired by or on behalf of the U.S. Government, then, as provided in FAR 12.212 and DFARS 227.7202-1 through 227.7202-4, as applicable, the U.S. Government's rights in the Software and its documentation shall be as specified in this Agreement. If any term or condition set forth in this Agreement:

- i. allows for the automatic termination of the Government's license rights or maintenance of services;
- ii. allows for the automatic renewal of services and/or fees;
- iii. allows for the Government to pay audit costs; and/or
- iv. requires the governing law to be anything other than Federal law, then such term and condition shall not apply to the U.S. Government but shall continue to apply to prime contractors and subcontractors of the Government.

Furthermore, nothing contained in this Agreement is meant to diminish the rights of the U.S. Department of Justice as identified in 28 U.S.C. Section 516. Finally, to the extent any term and condition set forth in this Agreement is contrary to U.S. Federal procurement law, then such term and condition shall not apply to the U.S. Government but shall continue to apply to prime contractors and subcontractors of the government.

q. WildFire: U.S. Government

Where End User is a U.S. Government contractor using or accessing WildFire: U.S. Government malware prevention service, End User certifies that now and so long as it uses or accesses WildFire: U.S. Government service:

- i. only U.S. citizens will be permitted to access WildFire: U.S. Government for administration and configuration;
- ii. End User holds an active contract or subcontract with the U.S. Federal Government and has a need to exchange e-mail, documents and other forms of communication with the U.S. Federal Government under a contract or subcontract;
- iii. End User shall cease using or accessing WildFire: U.S. Government when it no longer has an active contract or subcontract with the U.S. Federal Government; and
- iv. End User will abide by the confidentiality provisions contained within this Agreement.

SCHEDULE B.3. – PRICING

Managed Detection and Response & Professional Services for Michigan Public Safety
Communications System (MPSCS)

Operational Costs	
Term	10/1/2024 – 9/30/2025
ASTRO Managed Detection and Response w/ ATI	\$1,564,115.80
PremierOne MDR. Includes 100 EDR Licenses	\$36,687.04
ASTRO Support Services, Dispatch & Onsite Support	\$282,494.74
Total	\$1,883,297.58

One-Time Capital Costs	
System Integration Costs	
System Integration, Hardware, EDR Licensing & Training	\$1,122,861.35
Juniper Intrusion Detection Credit	\$120,000.00
Total	\$1,002,861.35

Professional Services	
NIST 800-53r5 SSP	\$340,720.00

Year 1 Total	
MPSCS Total	\$3,226,878.93

SCHEDULE R – PROFESSIONAL SERVICES ADDENDUM

This Professional Services Addendum (“PSA”) is PRIMARY AGREEMENT governed by the State of Michigan Contract No. 190000001544 dated October 1, 2019, as amended (“PRIMARY AGREEMENT”), entered into between Motorola Solutions, Inc. and the State of Michigan (“Customer”). PRIMARY AGREEMENT. Capitalized terms used in this PSA, but not defined herein, will have the meanings set forth in the PRIMARY AGREEMENT or the applicable Addenda.

- 1. Addendum.** This PSA governs Customer’s purchase of Professional Services (as defined below) and will form part of the Parties’ Agreement. This PSA will control with respect to conflicting or ambiguous terms in the PRIMARY AGREEMENT or any other applicable Addendum, but only as applicable to the Professional Services purchased under this PSA and not with respect to other Products and Services.
- 2. Professional Services; Applicable Terms and Conditions.**
 - 2.1. Professional Services.** Services provided by Motorola to Customer under this Agreement the nature and scope of which are more fully described in the Ordering Documents (“Professional Services”).
 - 2.2. Assessment of Systems & Operations.** If Customer is purchasing Professional Services to evaluate or assess networks, systems or operations, Customer acknowledges and agrees that the equipment provided by or used by Motorola to facilitate performance of the Services may impact or disrupt information systems. Except as specifically set forth in the Agreement, Motorola 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, and data, including, but not limited to, denial or 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. Motorola agrees to cooperate with Customer to schedule any such potential damage or disruption around Customer’s voice or information technology traffic and use patterns so as to reduce the risk of disruption during working hours.
 - 2.3. Network Security.** If Customer is purchasing network security assessment of network monitoring Professional Service, Customer acknowledges and agrees that Motorola does not guarantee or warrant that it will discover all of Customer’s system vulnerabilities or inefficiencies. Customer agrees not to represent to third parties that Motorola has provided such guarantee. Motorola disclaims any and all responsibility for any and all loss or costs of any kind associated with vulnerabilities or security events, whether or not they are discovered by Motorola.
 - 2.4. Application Development.** Reserved.

3. To obtain any additional Professional Services, Customer will issue a purchase order referring to this Agreement and the separate proposal document. Omission of reference to this Agreement in Customer's purchase order will not affect the applicability of this Agreement.
4. **Payment.** In accordance with the PRIMARY AGREEMENT.
5. **Survival.** The following provisions will survive the expiration or termination of this PSA for any reason: **Section 1 – Addendum; Section 2 – Professional Services; Applicable Terms and Conditions; Section 5– Survival.**

SCHEDULE S – DATA PROCESSING ADDENDUM FOR ASTRO AND PREMIER ONE MDR SERVICES

This Data Processing Addendum, including its Annexes (“DPA”), is governed by the State of Michigan Contract No. 190000001544 dated October 1, 2019, as amended (“Agreement”), entered into between Motorola Solutions, Inc. and the State of Michigan (“Customer”). **Unless otherwise agreed to by the parties, this DPA only applies to the Software and Services detailed in Schedule A - Attachment 12, Statement of Work.**

1. Definitions.

Capitalized terms used in this DPA, but not defined herein, will have the meanings set forth in the PRIMARY AGREEMENT or the applicable Addenda.

“**Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Regulatory frameworks may differ in their respective naming conventions and therefore may refer to a Controller as a Business or otherwise.

“**Data**” means collectively Motorola Data and Customer Data, including any Personal Data included therein.

“**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.

“**Processor**” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller. Processors act on behalf of the relevant Controller and under their authority. In doing so, they serve the Controller's interests rather than their own. Regulatory frameworks may differ in their respective naming conventions and therefore may refer to a Processor as a “Service Provider” or otherwise.

“**Security Incident**” means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration or disclosure of, or access to Customer Data, which may include Personal Data, while processed by Motorola.

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 the Agreement and Section 6 entitled “Sub-processors” below.
- 2.2. Motorola’s Processing of Customer Data.** See Schedule H. 7.3.1.
- 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 will 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 will 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 will 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 will not use the products and services in a manner that would violate applicable Data Protection Laws. Customer will 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.

3. Service Use Data. See Sch. H. 7.5.

- 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 will not, and will ensure its Authorized Users will not: (a) use the Motorola Data or Third-Party Data for any purpose other than Customer’s governmental 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. Any rights granted to Customer or Authorized Users with respect to Motorola Data or Third-Party Data will immediately terminate upon termination or expiration of the applicable addendum, order or the 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 will 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 the Agreement or applicable order

5. Motorola as a Controller or Joint Controller. In all instances where Motorola acts as a Controller it will comply with the applicable provisions of the Motorola Privacy Statement at Motorola Privacy Statement as each may be updated from time to time. Motorola holds all Customer Contact Data as a Controller and will Process such Customer Contact Data in accordance with the Motorola Privacy Statement.

6. Sub-processors.

6.1. Use of Sub-processors. See Sch. H. 7.3.3.

6.2. Changes to Sub-processing. The Customer hereby consents to Motorola engaging the list of Sub-processors as set forth in Annex III to process Customer Data provided that: (i) Motorola must provide thirty (30) days written prior notice of the addition or removal of any Sub-processor; (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 DPA and the Agreement; 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 will, 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 will provide Customer

with commercially reasonable cooperation and assistance in relation to any complaint, notice, or communication from a Data Subject. Customer will respond to and resolve promptly all requests from Data Subjects which Motorola provides to Customer.

7. Data Transfers

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

8. **Security.** Motorola will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks posed by the Processing of Customer Data which may include Personal Data. The appropriate technical and organizational measures implemented by Motorola are set forth in the PRIMARY AGREEMENT, including its Schedule P – Data Security Requirements, and in Annex II.

Security Incident Notification and Loss or Compromise of Customer Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, integrity, or availability of Customer Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of Customer Data, Contractor must, as applicable:

- (a) notify the State as soon as practicable but no later than 24 hours of becoming aware of such occurrence;
- (b) provide reasonable cooperation with the State in investigating the occurrence in a manner that does not interfere with Contractor’s mitigation and containment of any incident, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State;
- (c) in the case of PII or PHI, at the State’s sole election:
 - (i) with approval and assistance from the State, and if required by applicable law, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within 5 calendar days of the occurrence; or
 - (ii) reimburse the State for any costs in notifying the affected individuals;
- (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than 24 months following the date of notification to such individuals;
- (e) perform or take any other actions required to comply with applicable law as a result of the occurrence;

(f) pay for any costs associated with the occurrence to the extent of Contractor's responsibility for the incident, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution;

(g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence to the extent of Contractor's responsibility for the incident;

(h) be responsible for recreating lost Customer Data to the extent possible within a reasonable time frame without charge to the State; and

(i) provide to the State a detailed plan within a reasonable time frame describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. The State will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by the State in writing prior to its dissemination.

For purposes of clarity, "suspected to compromise" means a determination by Contractor based on specific and articulable facts and circumstances, taken together with rational inferences from those facts, that an act or omission may likely result in a breach of security, confidentiality, availability or integrity of the products and services provided hereunder of Customer Data.

The parties agree that any damages arising out of a breach of the terms set forth in this Section are to be considered direct damages and not consequential damages.

9. Data Retention and Deletion. See Sch. H. 7.4.

10. Regulation of Specific Terms.

10.1. 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 will comply with the terms of the CJIS Security Addendum for the Term of this Agreement. Motorola personnel that require access to unencrypted Criminal Justice Information ("CJI") for purposes of Tier 3 support (e.g. troubleshooting or development resources) must be escorted by a MPSCS Authorized User who is authorized unescorted CJI access.

In an emergency situation, MPSCS may provide escorted access via a mutually agreeable virtual method only if strictly necessary provided such access remains in compliance with CJIS requirements. In the event Customer requires access to Service Use Data for its compliance with the CJIS Security Policy, Motorola will make such access available following Customer's request. Notwithstanding the foregoing, in the event the Agreement or applicable ordering document terminates, Motorola will 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.

- 10.2. Data Protection Laws.** 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.
- 10.3. Motorola Contact.** If Customer believes that Motorola is not adhering to its privacy or security obligations hereunder, Customer will contact the Motorola Data Protection Officer at Motorola Solutions, Inc., 500 W. Monroe, Chicago, IL USA 90661-3618 or at privacy1@motorolasolutions.com.

SCHEDULE S – ANNEX I

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 offenses); or
- Any other personal data identified under applicable law or regulation.

Sensitive data transferred

To the extent that a solution sold under an Agreement requires the processing of sensitive personal information, it will be restricted to the minimum processing necessary for the solution functionality and be subject to technical security measures appropriate to the nature of the information.

The frequency of the transfer Data may be transferred on a continuous basis during the term of the 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 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 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 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 Agreement and applicable ordering documents. Any such Sub-processors will 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. For avoidance of doubt, the Software and Customer Data must be securely stored, hosted, supported, administered, Accessed, and backed up in the United States or its territories. The use of Offshore Resources is not permitted.

SCHEDULE S – ANNEX II

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

Measures of pseudonymization and encryption of personal data

Where technically feasible and when not impacting services provided: Motorola Solutions minimizes the data it collects to information it believes is necessary to communicate, provide, and support products and services and information necessary to comply with legal obligations. Motorola Solutions encrypts data in transit and at rest. Motorola Solutions pseudonymizes and limits administrative accounts that have access to reverse pseudonymization.

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 its information security practices 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

Motorola's availability and backup strategy is designed to ensure replication and fail-over protections in the event of a physical or technical incident. Personal Data is backed up and maintained using at least industry standard methods

Security Incident Procedures. Motorola 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 authorization

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 twelve 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, 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 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 treat that data as Motorola Solutions Confidential Restricted information.

Security and Privacy Awareness. Motorola ensures that its employees and contractors remain aware of industry standard security and privacy practices, and their responsibilities for protecting Customer Data, which may include Personal Data. This includes, but is not 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 will be periodically reviewed and include criminal background checks, proof of identity validation and any additional checks as deemed necessary by Motorola.

Measures for ensuring events logging

Motorola Solutions logs, or enables Customers to log, access and use of products or services that Process Customer Data. Logging of defined system activities, with appropriate event details, is required by Motorola Solutions policy. Such policy also requires integrated audit record review via a Security Information Event Management system and requirements for appropriate audit trail log management.

Measures for certification/assurance of processes and products

Motorola performs internal security evaluations such as Secure Application Reviews and Secure Design Review as well as Production Readiness Reviews prior to product or service release. Where appropriate, privacy assessments are performed for Motorola's products and services. A

risk register is created as a result of internal evaluations with assignments tasked to appropriate personnel. Security audits are performed annually with additional audits as needed. Additional privacy assessments, including updated data maps, may 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 the scope as set forth in its applicable certificate found at the Motorola Solutions Trust Center. .

Measures for ensuring data minimization

Motorola Solutions policies require processing of all personal information in accordance with applicable law, including when that law requires data minimization. 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 minimization.

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 industry standard frameworks including the Nymity Privacy Management and Accountability Framework, NIST Privacy Framework and ISO 27701. 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 Agreement, Motorola Solutions transfers Customer Data containing Personal Data to Sub-processors, such Sub-processors will be subjected to a security assessment and bound by obligations substantially similar, but at least as stringent, as those included in this DPA.

SCHEDULE S – ANNEX III

Sub-Processors

Motorola Solutions Sub-processors are identified below.

Applicable Sub-Processors:

1. Amazon.com, Inc
2. Google LLC
3. Okta
4. Palo Alto - US
5. ServiceNow
6. Tenable, Inc.
7. Twilio
8. Neustar

Optional Sub-Processor (Depending on contact methods)

9. PagerDuty, Inc



**STATE OF MICHIGAN
ENTERPRISE PROCUREMENT**

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **10**
to
Contract Number **MA190000001544**

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Various	Various
STATE	Contract Administrator	Nichole Harrell	DTMB
		517-449-9245	
		harrelln@michigan.gov	

CONTRACT SUMMARY				
MPSCS Continued System Updates, Equipment, Maintenance and Upgrades, and Ancillary Systems Products				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE	
October 1, 2019	December 31, 2029	0 - 0 Months	December 31, 2029	
PAYMENT TERMS		DELIVERY TIMEFRAME		
Net 45		As per Delivery Order.		
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
<input checked="" type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS				
No Minimum Delivery Requirements.				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$102,215,096.00	\$109,017,526.44	\$211,232,622.44		

DESCRIPTION

Effective December 17, 2024, the following changes are hereby incorporated into this Contract:

1. The parties add \$10,000,000.00 for public safety video systems detailed in the attached Schedule M - Statement of Work.
2. Andrew Richards (richardsa4@michigan.gov, 517-242-2560) has been added as a Program Manager for MSP.
3. The parties add \$99,000,000.00 for system and equipment updates and maintenance of the Michigan Public Safety Communication System.
4. The parties add \$17,526.44 for the completion of the Authority to Operate process for the VESTA-Motorola 9-1-1 compliant call handling software detailed in the attached statement of work.

All other terms, conditions, specifications, and pricing remain the same. Per Contractor and agency agreement, DTMB Central Procurement approval, and State Administrative Board approval on December 17, 2024.

**Program Managers
for
Multi-Agency and Statewide Contracts**

AGENCY	NAME	PHONE	EMAIL
MSP	Andrew Richards	517-242-2560	RichardsA4@michigan.gov
DTMB	Kate Jannereth	517-881-1031	JannerethK@michigan.gov
MSP	Jonathon Whitford	517-512-4068	WhitfordJ@michigan.gov

SCHEDULE M – STATEMENT OF WORK

Contract No. 171-190000000154

Public Safety Video Systems for Michigan State Police (MSP)

The Contractor will be held accountable to meet the requirements established in this Contract. The following revisions apply to this agreement with respect to Contract Change Notice No. 10, and do not apply or modify the existing agreement as a whole.

SCOPE

This Schedule includes:

1. Purchase of Public Safety Video Systems to include all Hardware, Software and all related components.
2. System Installation
3. System Training and materials.
4. System Warranty
5. System Maintenance

The State reserves the right to adjust products and services to fit their needs.

PROGRAM MANAGERS

The Program Managers for this work are identified as follows:

For MSP	For the Contractor
Andrew Richards Michigan State Police Headquarters Andrewsa4@michigan.gov 517-242-2560	Melanie Leenhouts Senior Account Manager Melanie.leenhouts@motorolasolutions.com 616-706-1723

Requirements

1.1. General Requirements

The Contractor must provide the following products as specified in Attachment 12, Pricing Additions:

1. Vehicle Mounted Video and Recording
2. Body Worn Video Recording Systems,
3. Interview Room Video and Recording
4. Video Storage, Security, Software and Peripherals

Equipment must meet all the listed specifications in Schedule D, Technical Requirements; be new, unused and in original unopened packaging.

1.2. Warranties

The Contractor must provide a manufacturer's warranty on all Hardware products. Refer to the following exhibits of this Statement of Work:

- Exhibit 2 – Hardware Warranties for Servers – Five Years
- Exhibit 3 – In-Car Hardware Warranty – Five Years
- Exhibit 4 – Wearable Camera Hardware Warranty – Two Years
- Exhibit 5 – Wearable Camera Extended Hardware Warranty – Three Years

1.3. Recall Requirements and Procedures

The Contractor must notify the State's Contract Administrator and agency Program Manager via email and phone call or message within one (1) business day of any recall or safety notices relating to all public safety video systems and components purchased under the Contract. In addition, this notice must be received in writing within three (3) business days, as specified in Section 26.5. Notices of this Contract.

The Contractor is responsible for providing return authorization and replacing or issuing credit for all products that are subject to recall at no additional charge to the Agency. Receipt of public safety video systems and components must occur within 15 calendar days from the date of this notification.

1.4. Transition

1. **Post-Contract Transition:** Invoices will be sent via email to the Agency Program Manager within 45 days after expiration of contract. Any invoices received after 45 days will result in a non-payment of invoice.

Service Requirements

1.5. Timeframes

All Contract Activities must be delivered within 30-45 calendar days from receipt of order. The receipt of order date is pursuant to the **Notices** section of the Standard Contract Terms.

1.6. Delivery

Contractor must deliver all Hardware and Software, within 30-45 calendar days from receipt of order, with the exception of optional parts which will be delivered within 8-10 business days upon receipt of order.

Delivery location will be specified on the Delivery Order (DO). The receipt of order date is pursuant to Section 26.5, Notices, of the Contract Terms.

Packaging must be optimized to permit the lowest freight rate. Shipments must be palletized whenever possible using manufacturer's standard 4-way shipping pallets.

The Contractor will utilize United Parcel Service (UPS) as the transportation method for delivery of the Contract Deliverables. All orders ship UPS ground. Expedited shipping is available for an additional fee. At MSP's request, Contractor will ship an order overnight for an additional \$100.00, or second day for an additional \$50.00. If there are extenuating circumstances, these fees may be modified or waived on a case-by-case basis. The Contractor will ship bulk (palletized) for the larger orders processed when shipping 20 or more in-car/wearable systems and/or some of the larger servers. Some Authorized Users may also require shrink wrapping. Authorized Users will inform Contractor of any such requirements.

All products should be shipped in a manner which enables the receiver to easily check shipment with the invoice. All individual units of measure (cases, rolls, pallets, etc.) should have a clearly visible “vendor product label” containing the following fields:

- a. Manufacturer Product Number
- b. Item Description
- c. Quantity per Unit of Measure

The State will use the acceptance process defined in Section 8, Acceptance Testing, Acceptance, of the Standard Contract Terms.

Prices are F.O.B. destination, within the State premises with transportation and handling charges paid by Contractor.

1.7. Installation

MSP will conduct the in-car hardware installations for the fleet of patrol vehicles. Contractor will provide MSP technician training of in-car hardware installation as specified in Section 2.7. Training.

On a case-by-case basis and as requested by State, Contractor may be required to perform in-car hardware installation per vehicle.

1.8. Specific Standards

1.8.1. IT Policies, Standards and Procedures

Contractors are advised that the State has methods, policies, standards and procedures that have been developed over the years. All services and products provided as a result of this agreement must comply with all applicable State IT policies and standards. Non-public PSPs are available to Contractor under NDA.

Public IT Policies, Standards and Procedures (PSP):

DTMB - IT Policies, Standards & Procedures (michigan.gov)

1.8.2. SOM Digital Standards

All software items provided by the Contractor must adhere to the State of Michigan Application/Site Standards which can be found at SOM Applications and Site Standards (michigan.gov).

1.8.3. Mobile Responsiveness

The Contractor’s Software must utilize responsive design practices to ensure the application is accessible via a mobile device.

1.8.4. ADA Compliance

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites and software applications. All websites, applications, software, and associated content and documentation provided by the Contractor as part of the Solution must comply with the Digital Accessibility Standards.

1.8.5. User Type and Capacity

Contractor must be able to meet the expected number of user licenses listed below:

Type of User License	Number of User Licenses
Body-Worn Camera	1,688
In-Car Video Systems	1,318

1.8.6. Access Control and Authentication

The Contractor’s Software must implement identity federation with the State’s MiLogin IT Identity and Access Management (IAM) environment as described in the State of Michigan Administrative Guide (1340.00.020.08 Enterprise Identity and Access Management Services Standard (michigan.gov).

To support federation with the SOM MiLogin Software, the Contractor’s Software must support SAML, OpenID or OAuth federated identity protocols. Software running within the States internally managed IT environment may be suitable for integration with the State’s Active Directory services as identified in the 1340.00.020.08 standard.

1.8.7. End-User Operating Environment

The SOM IT environment includes FedRAMP authorized major cloud providers and on-premises market leading virtualization environments, with supporting platforms that includes enterprise storage, monitoring, and management running in house and in cloud hosting provides.

Contractor must accommodate the latest browser versions (including mobile browsers) as well as some pre-existing browsers. To ensure that users are able to access online services, Contractor must ensure applications and websites display and function accurately in, at minimum, the two most recent major versions of the following browsers, without reliance on special plugins or extensions:

- Google Chrome
- Microsoft Edge
- Firefox
- Safari

Contractor must support the current and future State standard environment at no additional cost to the State.

1.9. Technical Support and Repairs

When providing technical support, the Call Center must resolve the caller’s issue within 60 minutes. If the caller’s issue cannot be resolved within 8 hours, on-site service must be scheduled. The on-site service must be performed within 24 hours of the time the issue was scheduled for service.

1.10. Maintenance

On-site maintenance must be performed according to the recommended manufacturer maintenance schedule.

1.11. Training

Training and knowledge sharing are important aspects of Contractor’s overall solution. Contractor’s goal is to help all stakeholders (officers, supervisors, system administrators, installers, etc.) to obtain a level of training required for their specific role. To achieve this goal, Contractor will conduct formal training classes

and provide useful reference documentation for the operation of the system. Additionally, Contractor's support staff will be available to assist 24 hour a day, seven days a week.

The training and handoff phase of implementation will last approximately two days depending on how MSP wants to structure training class attendance.

The following training is included the System Configuration specified in Schedule B Pricing, Implementation Services:

Class Name	Description	Participants	Class Size
End User Training	Training of MSP staff will take place onsite as needed for the in-car user experience and will take approximately 1 to 2 hours per class.	End-User / Officer	Up to 30
Admin Training	This classroom based comprehensive training includes camera user, administrative functions, troubleshooting, and Evidence Library configuration and management. The training will consume an entire day and can be section off, if needed by MSP, to isolate certain areas for certain users.	Supervisors and Administrative staff responsible for Evidence Library	Up to 20
Evidence Library User Training	This video or classroom-based training is intended to train users to search for and produce evidence.	Admin staff	N/A
Evidence Library Admin Training	This training is intended to train Information Technology support personnel on the operations aspects of the Evidence Library system and servers. This training can be provided onsite or via web session and is included with the Evidence Library installation.	IT staff	N/A
Online Training	Available with two courses: Basic Operation and using the Evidence Library software. These classes are self-paced and include an assessment at the end of each course. The results can be provided to Supervisors if needed. Providing a list of names and email addresses is all that is needed to sign up.	Determined by Department	N/A

Contractor must provide training materials and useful reference documentation accessible online for the operation of any Hardware and Software which must updated throughout the term of the Contract at no additional cost.

1.12. Reporting

The Contractor must submit electronically to the agency Program Manager within 10 days from the last day of every month a purchase history report of all purchases itemized by work site. Report will provide details of the description of product or services, including serial numbers, of all applicable parts, quantities, and costs. Within 30 calendar days of the Effective Date, the Contractor will submit a final report format to the agency Program Manager for final approval.

The State and/or Program Manager reserves the right to request additional reports, which shall be at no charge.

1.13. Meetings

The State may request meetings, as it deems appropriate.

Staffing

1.14. Key Personnel

The Contractor must appoint one Project Manager who will be directly responsible for the day-to-day operations of the Contract and other Key Personnel to support this Contract (“Key Personnel”). Key Personnel must be specifically assigned to the State account, be knowledgeable on the contractual requirements, and respond to State inquiries within one business day.

The Contractor may not remove or assign Key Personnel without the prior consent of the State. Prior consent is not required for reassignment for reasons beyond the Contractor’s control, including illness, disability, death, leave of absence, personal emergency circumstances, resignation, or termination for cause. The State may request a résumé and conduct an interview before approving a change. The State may require a 30-calendar day training period for replacement personnel.

Contractor Representative Contact Information:

Melanie Leenhouts
Senior Account Manager
Melanie.leenhouts@motorolasolutions.com
616-706-1723

Support Staff Contact Information:

1. For technical support, contact Mobile Video Technical Support at 800-605-6734, prompt #2 or send a technical request email to MobileVideoTechnicalSupport@motorolasolutions.com.
2. For repair requests, send an email to MVREPAIR@motorolasolutions.com.
3. The supported products include:
 - Body cameras: Vista series, V300, V700, VB400
 - In-car systems: DV1(EOL), 4RE, M500
 - Software: ELX(EOL), EL4, EL5, ELC

Trainer Contact Information:

Jason Bernard
Regional Sales Manager
Jason.bernard@motorolasolutions.com
616-889-1642

1.15. Customer Service Contact Information

The Contractor must specify its phone number for the State to make contact with the Contractor Representative who must be available for calls during the hours of 8:00 am to 5:00 pm EST Monday through Friday. In the event of an emergency after State business hours, the Contractor must provide a contact and phone number. The Contractor must respond to the State within two (2) hours of the emergency call.

Contractor Customer Service Contact Information:

1. For technical support, contact Mobile Video Technical Support at 800-605-6734, prompt #2 or send a technical request email to MobileVideoTechnicalSupport@motorolasolutions.com.
2. For repair requests, send an email to MVREPAIR@motorolasolutions.com.
3. The supported products include:
 - Body cameras: Vista series, V300, V700, VB400
 - In-car systems: DV1(EOL), 4RE, M500
 - Software: ELX(EOL), EL4, EL5, ELC

1.16. Technical Support, Repairs and Maintenance

The Contractor must specify its number for the State to contact the Contractor for technical support, repairs and maintenance. The Contractor must be available for calls and service during the hours of 8:00 AM to 5:00 PM EST Monday through Friday, at a minimum. In the event of an emergency after State business hours, the Contractor must provide a contact and phone number for technical support, repairs, and maintenance. The Contractor must respond to the State within two hours of the emergency call.

Contractor Contact Information:

Motorola Solutions strives to have the best service team in the industry through delivering thorough and efficient customer service. We continually ensure our representatives are available 24 hours a day, seven days a week through the following options:

1. Submit and manage support tickets and RMA requests, chat with an agent, as well as explore learning modules and documentation all through our Customer Hub portal at <https://customerhub.motorolasolutions.com>.
 - a. If you have any questions about how to access Customer Hub, please reach out to portal.support@motorolasolutions.com.
2. A technical support representative can be reached by dialing our toll-free support number: 1 (800) MSI-HELP. You can then say what you are calling into support about, such as Parts, RMA, or Technical Support. Our voice recognition system will then route you to the appropriate team.
3. Submit a technical support request via email at: mobilevideotechnicalsupport@motorolasolutions.com.
 - a. Please include your agency name, a point of contact's name and contact information, site ID, and a description of your request.

Technical Support: The Technical Support Team provides initial support and troubleshooting for tickets. It can also escalate tickets if additional support is needed.

Hours: Monday - Friday (7:00 AM to 6:00 PM Central); Tickets are answered via Pager during Holidays & After-Hours

Voice Prompts: "Technical Support Mobile Video"

Repair Team: The Repair Team manages all return material authorization requests, FLIP repairs, and provides replacements for pieces of equipment such as DVR, body cameras, etc. The team also provides case statuses for repair orders and missing/wrong parts, as well as sales representative contact information for out-of-warranty upgrades. If you have any questions or would like to receive updates, you can email mobilevideorepair@motorolasolutions.com.

Hours: Monday - Friday (7:00 AM to 6:00 PM Central); Tickets are answered via Pager during Holidays & After-Hours

Voice Prompts: "RMA Mobile Video" or "Repairs Mobile Video"

1.17. Disclosure of Subcontractors

The Contractor will not be utilizing subcontractors.

1.18. Security

The Contractor will be subject to the following security procedures: All personnel accessing criminal justice information systems or facilities are required to pass a fingerprint-based background check. Any criminal convictions may result in the Contractor being refused access to the facility.

In addition, fingerprint background checks are required for any technician requiring remote access. These technicians, if allowed remote access into MSP's Contractor solution, will utilize security tokens and authentication procedures as instructed by MSP and the Department of Technology, Management and Budget (DTMB).

The State may require the Contractor's personnel to wear State issued identification badges.

Pricing

1.19. Price Term

Pricing is firm for the entire length of the Contract.

1.20. Price Changes

Adjustments will be based on changes in actual Contractor costs. Any request must be supported by written evidence documenting the change in costs. The State may consider sources, such as the Consumer Price Index; Producer Price Index; other pricing indices as needed; economic and industry data; manufacturer or supplier letters noting the increase in pricing; and any other data the State deems relevant.

Following the presentation of supporting documentation, both parties will have 30 days to review the information and prepare a written response. If the review reveals no need for modifications, pricing will remain unchanged unless mutually agreed to by the parties. If the review reveals that changes are needed, both parties will negotiate such changes, for no longer than 30 days, unless extended by mutual agreement.

The Contractor remains responsible for Contract Activities at the current price for all orders received before the mutual execution of a Change Notice indicating the start date of the new Pricing Period.

Ordering

1.21. Authorizing Document

The appropriate authorizing document for the Contract will be a Delivery Order (DO) referencing this Master Agreement (MA) or a procurement card transaction.

Orders under \$5,000.00 for replacement parts and accessories may be placed by procurement card by authorized individuals.

1.22. Order Verification

The Contractor must have internal controls, to verify abnormal orders and to ensure that only authorized individuals place orders and that non-State public entities are current MiDeal members

www.michigan.gov/mideal.

Acceptance

1.23. Acceptance, Inspection and Testing

The State will use the acceptance process defined in Section 8, Acceptance Testing, Acceptance, of the Standard Contract Terms.

Invoice and Payment

1.24. Invoice Requirements

All invoices submitted to the State, as specified on the Purchase Order/Delivery Order, must include the following:

- (a) Date
- (b) Invoice Number
- (c) Contract Number/Master Agreement Number
- (d) Purchase Order/Delivery Order
- (e) Quantity
- (f) Description of product (including serial number) and services
- (g) Name of person placing order
- (h) Unit Price
- (i) Discounts or Credits
- (j) Billing Address
- (k) Shipping Address

Only properly submitted invoices will be officially processed for payment.

1.25. Payment Methods

The State will make payment for Contract Activities via Electronic Funds Transfer (EFT).

Licensing Agreement

The Contractor must provide a copy of any applicable licensing agreement.

Additional Requirements

1.26. Hazardous Chemical Identification

In accordance with the federal Emergency Planning and Community Right-to-Know Act, 42 USC 11001, et seq., as amended, the Contractor must provide a Material Safety Data Sheet listing any hazardous chemicals as defined in 40 CFR §370.2, to be delivered. Each hazardous chemical must be properly

identified, including any applicable identification number, such as a National Stock Number or Special Item Number.

The Contractor must identify any hazardous chemicals that will be provided under any resulting contract.

1.27. Mercury Content

Pursuant to MCL 18.1261d, mercury-free products must be procured when possible. The Contractor must explain if it intends to provide products containing mercury, the amount or concentration of mercury, and whether cost competitive alternatives exist. If a cost competitive alternative does exist, the Contractor must provide justification as to why the particular product is essential. All products containing mercury must be labeled as containing mercury.

1.28. Brominated Flame Retardants

The State prefers to purchase products that do not contain brominated flame retardants (BFRs) whenever possible. The Contractor must disclose whether the products contain BFRs. Contractor must describe how products that meet these requirements are identified or otherwise labelled.

The Contractor has disclosed that the provided products do contain small amounts of Brominated Flame Retardants, which has been identified thru laboratory analysis of the products.

1.29. Perfluoroalkyl and Polyfluoroalkyl Substances (PFAS)

The Contractor must confirm that the provided products do not intentionally contain PFAS. This consists of all components of the provided products, including product packaging.

Additional Information

The State reserves the right to purchase any additional services or products from the Contractor during the duration of the Contract, subject to Contractor's approval and such will be documented in writing and signed as a Contract Change Notice by an authorized representative of both parties.

SCHEDULE M – EXHIBIT 1 – BUSINESS TECHNICAL WORKSHEET

Contractor will meet each Business Technical Requirement as stated herein.

1. General Hardware/Software Requirements

#	Requirement	MSI Response:
1.1	Contractor's System must have controlled access to video evidence, define roles, permissions, users and passwords.	Comply
1.2	Contractor's System must include a complete audit trail with any access, modification, deletion, or export action recorded within the audit trail. The audit trail must include date, time, user and action performed.	Comply
1.3	Contractor's System must have the capability to create multiple event labels, tags, markers, and clips without altering the original video files.	Comply
1.4	Contractor's System must have the ability to search all video files within the Contractor's solution, with access adjusted by permissions and roles.	Comply
1.5	Contractor's System must have a secure method to access the camera system to prevent any unauthorized access to recording device data.	Comply
1.6	Digital video file of the Contractor's System must provide ability to determine and authenticate an original file or indicator file has been modified.	Comply
1.7	In case of system failure or damage, Contractor must provide a method to recover video and data files, at no additional cost to the State. If a camera system experiences a failure or is damaged, the State will ship the camera system to Contractor's headquarters. Once received, the Contractor's recovery team will extract the files and send them back to the State on a storage drive, at no additional cost to the State.	Comply
1.8	Contractor's System must have fleet management settings with manual and wireless options for installing VRS firmware or updating configurations. Device firmware must be included free of charge.	Comply
1.9	Contractor's System must have the ability to export video in a nonproprietary format, with no proprietary file players required to view the video.	Comply
1.10	Contractor's System must have the ability to export to physical media (i.e. DVDs, Blu-Ray, and USB thumb drive).	Comply
1.11	Contractor's System should have the optional ability to integrate with Microsoft Active Directory	Comply
1.12	Contractor's System must have redactive capabilities.	Comply

2. In Car Camera Requirements:

Screen/Monitor

#	Requirement	MSI Response:
2.1	Must have a display/control center (separate from Mobile Data Computer) minimum 3 inches / maximum 6 inches diagonal with color display.	Comply
2.2	Must have a display/control center (separate from Mobile Data Computer) minimum 3 inches / maximum 6 inches diagonal with color display.	Comply
2.3	Field review and labelling of historical videos from control center.	Comply
	Display	
2.4	User controlled brightness dimming (from full brightness to off) and “covert” mode to turn off all display indicators/lights while maintaining record status.	Comply
	Temp Range	
2.5	Monitor should include a non-glare touchscreen or mechanism to control video in the vehicle.	Comply
	Display Viewing Angle / Dlag.	
2.6	Sub Zero to 120 Degrees Fahrenheit	Comply
	Microphone	
2.7	Rotation of 360 Degrees or 180 front facing	Comply
2.8	Wireless audio from range of 1000 feet with bi-directional record activation of audio and video.	1000' Line of sight. “Operating range varies according to environmental conditions and installation”.
2.9	12-hour record time battery life with recharge options inside the patrol vehicle	Comply
	Product must have low battery indicators provide process for system to power down without causing any damage to recording device or video storage unit.	Comply
2.11	Mute option on wireless mic.	Comply
2.12	“Covert” mode option to silence all lights/sounds.	Comply
2.13	Full 2.25” Sam Browne duty belt clip or belt pouch, without requiring uniform modifications.	Comply
2.14	Subzero to 100 Degrees Fahrenheit operation	Exceed

#	Requirement	MSI Response:
2.15	Wireless mic must indicate loss of sync/connection with VRS.	Comply
2.16	If properly synced with VRS, must not lose sync due to loss of range or temporary loss of power (i.e. – Audio must resume when user is back in range, without a manual sync operation).	Comply
2.17	Replaceable battery	
2.18	VRS must allow sync of 2 wireless microphones or up to 8 body worn cameras.	Comply
	Activation	
2.19	Wireless mic must have an option for a lapel (remote) mic.	Comply
2.20	Product must power on with the vehicle ignition and record a triggered event independent of a user login. Record Button, Emergency Lights, Speed, Collision, wireless microphone, body worn camera activation, and/or Siren. Activation and recording must occur without MDC requirements.	Comply
	Sensors	
2.21	The VRS must activate recording if triggered, regardless of any action or menu shown on the control center, during normal use. This requirement may not apply to a technician’s diagnostic troubleshooting mode.	Comply
	Buffering	
2.22	There must be sensors to collect the status of the siren, brakes, speed of patrol car, VRS record status, body worn camera and microphone audio status in the metadata/on video file. There should be a method to display the status indicators during playback.	Comply
	Collision	
2.23	Pre-event buffering and continuous background video buffering.	Comply
	Duration	
2.24	There must be a method to ensure there is not a complete loss of video due to a collision. (e.g.-battery backup) This method should guarantee system fidelity except in the event of complete physical VRS storage destruction, due to the collision. Activate and record with pre-event in case of patrol car collision.	Comply
2.25	Record individual events uninterrupted for minimum of 3.5 hours	Comply
	Record Indicators	
	Front Camera Lens	

#	Requirement	MSI Response:
2.26	Illuminated indicator visible outside and to front seat	Comply
2.27	Autofocus/Auto exposure; auto white balance, if applicable. Lens may be fixed or zoom capable.	Comply
	Internal Camera Lens	
2.28	While interior camera is recording, front camera must also continue to record.	Comply
2.29	480 SD recording with infrared night vision recording	Comply
	Internal Microphone	Comply
2.30	Must be capable of recording both interior front seats.	Comply
	Erasure Prevention	
2.31	Internal camera activation must be separate from external camera activation, configurable to be controlled (triggered) by the user, or configurable to be on by default.	Comply
	Time Stamp	
2.32	Must record interior microphone when interior camera is active. User must be able to mute internal microphone. VRS must display an indicator of audio status (mute or recording) of microphones.	Comply
	Audit Log	
2.33	Erasing, Altering, and/or Recording over event video data.	Comply
	Equipment Diagnostic	
2.34	Video, Audio, Metadata must be consistent	Comply
2.35	Name/ID, automated verification of hashed data, access/views, edits, exports, archive status, purge/deletion	Comply
2.36	Must perform self-test to complete functionality.	Comply
	Download	
2.37	Storage Space or Record Time Remaining must be visible	Comply
	Front Camera Field of View	
2.38	57 degrees	Exceed
	High-Definition Field of View	

#	Requirement	MSI Response:
2.39	720p/30fps and option for lower resolution recording as set by system administrators	Exceed
	Equipment Mounts	
2.40	Product must be a complete mountable solution to accommodate different types of patrol vehicles, (i.e. Ford Interceptor and SUV, Dodge Durango and Chargers, Chevrolet Tahoe).	Comply
2.41	Product must not interfere with normal operation of the emergency vehicle; and must not create a safety risk for operators or passengers. Must not cause interference with any other electronic systems in operation (radio, computer, speed detection, etc.)	Comply
	Video / Audio Recordings	
2.42	System recording should be in a nonproprietary video format. Recording should be both audio and video, with separate channels and capabilities of recording events inside and outside the vehicle simultaneously.	Comply
	Internal Storage	
2.43	64 GB	Exceed

3. Body Worn Camera Requirements

Screen / Monitor

#	Requirement	MSI Response:
3.1	Control center must allow event category and report number labelling.	Comply
3.2	Field review and labelling of historical videos from control center.	Comply
	Display	
3.3	User controlled brightness dimming (from full brightness to off) and “covert” mode to turn off all display indicators/lights while maintaining record status.	Comply
	Temp Range	
3.4	Sub Zero to 120 Degrees Fahrenheit	Exceed
	Display Viewing Angle / Dlag.	
3.5	130 Degrees Field of View	Comply
	Microphone	

#	Requirement	MSI Response:
3.6	Wireless audio from range of 1000 feet with bi-directional record activation of audio and video.	1000' Line of sight. "Operating range varies according to environmental conditions and installation".
3.7	12 hours HD or 13 hours SD record time battery life with recharge options inside the patrol vehicle	Exceed with Swappable Battery
3.8	Mute option on wireless mic.	Comply
3.9	"Covert" mode option to silence all lights/sounds.	Comply
3.10	Full 2.25" Sam Browne duty belt clip or belt pouch, without requiring uniform modifications.	Comply
3.11	Wireless mic must indicate loss of sync/connection with VRS.	Comply
3.12	If properly synced with VRS, must not lose sync due to loss of range or temporary loss of power (i.e. – Audio must resume when user is back in range, without a manual sync operation).	Comply
3.13	Replaceable battery	Comply
3.14	VRS must allow sync of 2 wireless microphones or 8 body worn cameras.	Comply
3.15	Wireless mic must have an option for a lapel (remote) mic.	Comply
3.16	Product must have low battery indicators provide process for system to power down without causing any damage to recording device or video storage unit.	Comply
	Activation	
3.17	Record Button, Emergency Lights, Speed, Collision, wireless microphone, body worn camera activation, and/or Siren. Activation and recording must occur without MDC requirements.	Comply
3.18	The VRS must activate recording if triggered, regardless of any action or menu shown on the control center, during normal use. This requirement may not apply to a technician's diagnostic troubleshooting mode.	Comply
	Sensors	
3.19	There must be sensors to collect the status of the VRS record status, body worn camera, and microphone audio status in the metadata/on video file. There should be a method to display the status indicators during playback.	Comply
	Buffering	

#	Requirement	MSI Response:
3.20	Pre-event buffering and continuous background video buffering.	Comply
	Collision	
3.21	Activate and record with pre-event in case of patrol car collision.	Comply
	Duration	
3.22	Record individual Events uninterrupted for minimum of 3.5 hours.	Comply
	Record Indicators	
3.23	Illuminated indicator visible outside and to front seat	Comply
	Front Camera Lens	
3.24	Autofocus/Auto exposure, auto white balance, if applicable. Lens may be fixed or zoom capable.	Comply
	Erase Prevention	
3.25	Erasing, Altering, and/or Recording over event video data.	Comply
	Time Stamp	
3.26	Video, Audio, Metadata must be consistent	Comply
	Audit Log	
3.27	Name/ID, automated verification of hashed data, access/views, edits, exports, archive status, purge/deletion	Comply
	Equipment Diagnostic	
3.28	Must perform self-test to complete functionality.	Comply
3.29	Storage Space or Record Time Remaining must be visible	Comply
3.30	Must send notification to user for any malfunction	Comply
	Download	
3.31	Must have wireless and manual download capabilities	Comply
	High-Definition Resolution	
3.32	720p/30fps and option for lower resolution recording as set by system administrators	Exceed

#	Requirement	MSI Response:
	Audio / Video Recordings	
3.33	System recording should be in a nonproprietary video format. Recording should be both audio and video, with separate channels and capabilities of recording events inside and outside the vehicle simultaneously.	Comply
	Internal Storage	
3.34	32 GB	Exceed
	Wi-Fi and GPS	
3.35	Must have built-in Wi-Fi and GPS	Comply
	Integrate with In Car VRS	
3.30	Must fully integrate with in-car VRS	Comply
	Smart Device Access	
3.30	Manage features, categorize events and stream live video	Comply

SCHEDULE M - EXHIBIT 2 – IN CAR HARDWARE WARRANTY

Motorola Solutions M500 In Car Video System Warranties

1. Limited Warranty

Motorola Solutions, Inc. (“Motorola Solutions”) warrants each in-car camera system, part, and component it manufactures first sold to an end user to be free from defects in material and workmanship for a period of ONE-YEAR from the date of purchase. A defective component that is repaired or replaced under this limited warranty will be covered for the remainder of the original warranty period. Where defects in material or workmanship may occur, the following warranty terms and conditions apply:

Warrantor

This warranty is granted by Motorola Solutions, Inc., 415 E Exchange Parkway, Allen, TX75002, Telephone: 972-423-9777, Facsimile: 972-383-9661.

Parties to Whom Warranty Is Intended

This warranty extends to the original end user of the equipment only and is not transferable. Any exceptions must be approved in writing from Motorola Solutions.

Parts and Components Covered

All parts and components and repair labor of the warranted unit manufactured and/or installed by Motorola Solutions are covered by this warranty, except those parts and components excluded below.

Parts and Components Not Covered

The Limited Warranty excludes normal wear-and-tear items such as frayed or broken cords, broken connectors, and scratched or broken displays. Motorola Solutions reserves the right to charge for damages resulting from abuse, improper installation, or extraordinary environmental damage (including damages caused by spilled liquids) to the unit during the warranty period at rates normally charged for repairing such units not covered under the Limited Warranty. In cases where potential charges would be incurred due to said damages, the agency submitting the system for repairs must be notified. Altered, damaged, or removed serial numbers results in voiding this Limited Warranty. If while under the warranty period, it is determined that the Motorola Solutions system was internally changed, modified, or repair attempted, the system warranty will become null and void.

Limited Liability

Motorola Solutions’ liability is limited to the repair or replacement of components found to be defective by Motorola Solutions. Motorola Solutions will not be liable for any indirect, consequential, or incidental damages arising out of the use of or inability to use the system even if the unit proved to be defective. Motorola Solutions will not be responsible for any removal or re-installation cost of the unit or for damages caused by improper installation.

Remedy

If, within the duration of this warranty, a unit or component covered by this warranty is determined by Motorola Solutions to be defective in material or workmanship, Motorola Solutions shall replace any defective components. Replacement of a defective component(s) pursuant to this warranty shall be warranted for the remainder of the warranty period applicable to the system warranty period. Motorola Solutions will advance ship a replacement unit, or at the request of the customer, ask for the unit to be sent in for repair. In the case of an advanced shipment replacement, Motorola Solutions will supply a return label with the advance unit, and the customer must return the defect within thirty days.

Shipping

When an advanced replacement is sent out, the unit will ship via ground shipping, and Motorola Solutions will provide a prepaid shipping label to return any defective unit for end users in the continental United States. A serial number is required to be submitted with the request in order to receive an advanced replacement unit. The customer will need to contact Motorola Solution’s Customer Service Department to request a return material authorization (RMA) number. Failure to return the unit within the thirty-day window will result in the customer being billed the full purchase price of the advance shipped unit.

If the customer requests the unit be sent in for repair, the end user will be responsible for any shipping charges to Motorola Solutions. Motorola Solutions will return ship the product to a customer within the continental United States by prepaid ground shipping only. Any expedited shipping costs are the responsibility of the end user.

Customers that are outside the continental United States will be responsible for all transportation costs both to and from Motorola Solutions’ factory for warranty service, including without limitation to any export or import fees, duties, tariffs, or any other related fees that may be incurred during transportation. You may also obtain warranty service by contacting your local Motorola Solutions Authorized Service Center (ASC) for shipping instructions. A list of local ASCs may be obtained by contacting Motorola Solutions’ Customer Service Department. Customers will be responsible for all transportation costs to and from the local ASC for warranty service.

Extended Warranty

Extended Warranties may be purchased directly from Motorola Solutions. Any and all extended warranties must be purchased prior to the expiration of any previous warranty. Failure to purchase an extended warranty prior to the expiration of the warranty period will require the covered unit to be physically inspected at the facility of the manufacturer and any repairs necessary to bring the unit back to full working order must be performed prior to the issuance of any new warranty. The customer will be responsible for the cost of the inspection (equal to one hour of labor) plus the standard costs associated with any required repairs.

2. “Video-as-a-Service” Warranty

High Level Warranty Replacement Term Length	
In-Car Video system, part, and component	Every 3 to 5 Years

In-Car Camera Warranty

In car video warranties cover the duration of the contract, and additional sixth- or seventh-year warranties can be purchased as needed.

Motorola warrants each camera system, part, and component it manufactures first sold to an end user to be free from defects in material and workmanship for a period of five years from the date of purchase. A defective component that is repaired or replaced under this limited warranty will be covered for the remainder of the original warranty period. Where defects in material or workmanship may occur, the following warranty terms and conditions apply:

Warrantor

This warranty is granted by Motorola Solutions, Inc., 415 E Exchange Parkway, Allen, TX 75002. Telephone: 1-800-MSI-HELP.

Parties to Whom Warranty Is Intended

This warranty extends to the original end user of the equipment only and is not transferable. Any exceptions must be approved in writing from Motorola.

Parts and Components Covered

All parts and components, including consumable items such as batteries, and repair labor of the warranted unit manufactured and/or installed by Motorola are covered by this warranty, except those parts and components excluded below.

Parts and Components Not Covered

The Limited Warranty excludes camera mounts and normal wear-and-tear items such as frayed or broken cords and scratched or broken displays. Motorola reserves the right to charge for damages resulting from abuse, improper use, or extraordinary environmental damage (such as submersion in liquid) to the unit during the warranty period at rates normally charged for repairing such units not covered under the Limited Warranty. In cases where potential charges would be incurred due to said damages, the agency submitting the system for repairs MUST be notified. Altered, damaged, or removed serial numbers results in voiding this Limited Warranty. If while under the warranty period, it is determined that the Motorola system was internally changed, modified, or repair attempted, the system warranty will become null and void.

Limited Liability

Motorola's liability is limited to the repair or replacement of components found to be defective by Motorola. Motorola will not be liable for any indirect, consequential, or incidental damages arising out of the use of or inability to use the system even if the unit proved to be defective.

Remedy

If, within the duration of this warranty, a unit or component covered by this warranty is diagnosed by Motorola's Customer Service phone support and proves to be defective in material or workmanship, Motorola shall replace the defective unit with an Advance Replacement unit. The Advance Replacement unit will ship via UPS ground and include a prepaid shipping label to return the defective unit, which must

be received by Motorola within thirty days. The Advance Replacement unit pursuant to this warranty shall be warranted for the remainder of the warranty period.

Shipping

When an advance replacement is sent out, the unit will ship via ground shipping, and Motorola will provide a prepaid shipping label to return any defective unit for end users in the continental United States. A serial number is required to be submitted with the request in order to receive an advance replacement unit. The customer will need to contact Motorola's Customer Service Department to request a return material authorization (RMA) number. Failure to return the unit within the thirty-day window will result in the customer being billed the full purchase price of the advance shipped unit.

If the customer requests the unit be sent in for repair, the end user will be responsible for any shipping charges to Motorola. Motorola will return ship the product to a customer within the continental United States by prepaid ground shipping only. Any expedited shipping costs are the responsibility of the end user.

Customers that are outside the continental United States will be responsible for all transportation costs both to and from Motorola's factory for warranty service, including without limitation any export or import fees, duties, tariffs, or any other related fees that may be incurred during transportation. You may also obtain warranty service by contacting your local Motorola Authorized Service Center (ASC) for shipping instructions. A list of local ASCs may be obtained by contacting Motorola's Customer Service Department. Customers will be responsible for all transportation costs to and from the local ASC for warranty service.

SCHEDULE M – EXHIBIT 3 – WEARABLE CAMERA HARDWARE WARRANTY

Essential Service for V700 Body Worn Camera Device

1. Essential Service for V700 Body Worn Camera Device

1.1. Description of Services and Obligations

The term “Customer” refers to any end-user who has a purchase agreement with Motorola.

Essential Service provides either three (3) or five (5) years of coverage, as selected by the Customer, and includes:

- Remote Technical Support.
- Software Maintenance.
- Software Enhancements.
- Hardware Repair for manufacturing defects.

Motorola includes three (3) years of Essential Service with each Body Worn Camera (BWC) device purchase, with optional service upgrades to extend and/or provide additional coverage for the device.

1.2. Essential Service

1.3. Remote Technical Support

Remote Technical Support is provided for device issues related to software and/or hardware that require troubleshooting expertise. Motorola’s System Support Center (SSC) and Technical Support Operations (TSO) center are staffed with highly trained technologists who specialize in the diagnosis and resolution of product issues. Motorola’s SSC and TSO are continuously monitored against stringent, industry recognized incident and problem management processes.

Motorola will respond to calls, e-mails, and web portal submissions during normal support hours, five (5) business days per week, excluding holidays, and weekends. In addition, Customers may contact the Motorola Service Desk and a Motorola representative will log a technical request on Motorola’s Case Management System.

1.4. Technical Problem Isolation, Analysis and Resolution

A Motorola representative or technologists will:

- Work to isolate the problem/issue.
- Analyze and determine the cause of the problem/issue.
- Work to achieve problem/issue resolution.

1.5. Software Maintenance

Software maintenance is important for ensuring device performance and operation. Essential Service provides the Customer with access to the latest available Body Worn Camera (BWC) device operating

system (OS) software, device firmware, and application software. Device software releases maintain the device software performance such that the Device operates in accordance with its specifications and documented functionality and is aligned with the applicable Motorola infrastructure platform lifecycle. Each release may include bug fixes, security patches, and/or new feature activation enablement's.

Configuration of the Body Worn Camera (BWC) device is made possible through the use of the VideoManager EL On-Premise, or VideoManager EL Cloud, solution.

Access to software updates will remain available until the expiration of the initial term of the Essential Service Package. Upon expiration of the initial Essential Service term, availability of software updates will terminate, unless the Customer renews Essential Service.

1.6. Software Enhancements

Software Enhancements are included with all BWC devices that have a valid Essential Service Package. Software Enhancements may include, or introduce, new device features, functionality, or capabilities, that were not available at time of device purchase. Availability of software enhancements depends on the device hardware and software capability to work with the new enhancements. Certain enhancements, not included with Essential Service Packages, may only be available as an additional purchase.

Motorola, at its discretion, reserves the right to add new software enhancements, or remove existing software enhancements, from any of its Essential Service Package. Please contact your Motorola Sales associate, or visit the Motorola's Web portal, for additional information regarding device features and capabilities.

Software Enhancements for the device will be continuously available until the expiration of the initial term of the Essential Service Package. Upon expiration of the initial term of Essential Service, availability of Software Enhancements will terminate, unless the Customer renews Essential Service.

1.7. Device Hardware Repair

Essential Service provides the Customer with repair services at a Motorola owned and operated, supervised, or certified Repair Center that employs the latest test equipment and original or certified replacement components used in the manufacturing of the BWC device. Device Hardware Repair provides the Customer with repair services for internal and external device components that are damaged as a result of manufacturing defects and defects due to normal wear and tear. With this Service, the device is repaired to ensure full compliance with its specifications, as published by Motorola at the time of delivery of the original device via:

- Repairs, adjustments and restorations, if appropriate, of any device that malfunctions while being used within the operational and environmental parameters specified by Motorola.
- Device updates, if applicable, as may be released, from time to time, by Motorola in accordance with an Engineering Change Notice.

At the discretion of Motorola, if the device is considered "un-repairable", for technical or economic reasons, Motorola will replace the device with a new or refurbished device.

1.8. Essential Software Service

If for any reason the Customer declines or chooses to exclude the hardware repair option that is included with the three (3) year Essential Service Package, the Customer will automatically default to, and be entitled to, three (3) years of Essential Software Service and one (1) year of hardware repair against manufacturing defects, as covered by the standard product warranty.

Essential Software Service provides three (3) years of coverage and includes:

- Remote Technical Support.
- Software Maintenance.
- Software Enhancements.

1.9. Scope of Products or Services Included

Essential Service, and optional Service upgrades, are currently available for all V700 Body Worn Camera devices. Check with your Motorola's Sales representative if you have a question about the eligibility of your device.

Motorola Solutions Responsibilities

Software Release Availability. Motorola will provide access to the latest BWC device software and firmware releases via the VideoManager EL On-Premise, or VideoManager EL Cloud, solution. For customers using the VideoManager EL Cloud, software and firmware upgrades will occur automatically when the Body Worn Camera device connects to the agency's VideoManager EL Cloud instance. If using the VideoManager EL On-Premise solution, the on-prem server will periodically connect to the VideoManager EL Cloud database to check for new software and firmware versions, download the latest version, and apply the new software and/or firmware automatically to the BWC device when it connects to the server.

Software Release Notes. Motorola may, from time to time, provide release notes for the BWC Device software release. Information regarding training material **will be posted on the Learning Experience Portal (LXP) at <https://learning.motorolasolutions.com>**.

Hardware Repair. Motorola will provide repair or replacement of a device, at its option, with a five (5) business day in-house turnaround time, provided the device is delivered to the repair center by 9:00 a.m. (local repair center time), and replacement parts, components, and/or devices are available. Business days do not include holidays or weekends. Repair may include the replacement of parts, or boards with new parts or complete boards or, at Motorola's option, with functionally equivalent, reconditioned parts, boards, or with a new or refurbished replacement device. All replaced parts, boards or devices will become the property of Motorola. Turnaround time represents the time a product spends in the repair process; it does not include time in transit, including customs clearance.

LTE/4G Service. Motorola supports the operation of the V700 BWC device on multiple approved LTE/4G Carrier Networks. Based on the Customer's selection of a Carrier during the initial ordering process, Motorola will install, in the device, the Customer's selected Carrier SIM, before the device is shipped to the Customer. The Customer is responsible for contacting the Carrier and activating the LTE/4G data service.

Shipping. For devices repaired under Essential Service, Motorola will provide one-way shipping, from an Authorized Motorola Repair Center to the Customer. The Customer is responsible for the shipping method

and any shipping costs incurred when returning the faulty device to an Authorized Motorola repair center. Based on the country of purchase, Motorola may also cover, or include, two-way shipping for the damaged or defective device. Eligibility for two-way shipping will be confirmed during the repair submission process.

Customer Responsibilities

Serial Numbers. If device orders are submitted via Motorola's Partner Hub, OCC, or CPQ ordering systems, the hardware serial number(s) for three (3) year Essential Service and Essential Software, as well as five (5) year Essential Service, and three (3) and five (5) year Essential Service with Accidental Damage and Advanced Replacement, will be automatically captured and included in the Service Agreement.

If five (5) year Essential Service or three (3) and five (5) year Essential Service with Accidental Damage and Advanced Replacement is purchased within 90 days of device shipment, the Customer must provide a complete list, preferably in electronic format, or by completing a Service Order Form (SOF), of all hardware serial numbers to be covered under the Agreement.

Initiating Repair. When initiating a repair, the Customer must contact Motorola to obtain a Return Material Authorization (RMA) number for each faulty BWC device. The Customer can submit a repair, and request an RMA, via the Partner Hub Portal, or by contacting the Motorola's Service Desk. If two-way shipping is included, the customer can generate a shipping label via Partner Hub, or by contacting the Motorola Service Desk. The Return Material Authorization (RMA) must be included with the device when shipped to the Authorized Motorola Repair Center.

- Only the BWC device should be returned for repair. The battery must be removed before shipping the device to a Motorola Repair Center.
- Device accessories should not be included when returning a device to a Motorola Repair Center for repair. Accessories include batteries, chargers or charging stations, cables, mounts, and clips.
- The SIM card must remain in the device, and intact, when the device is shipped to a Motorola Repair Center. If the SIM card is removed, or if any evidence of SIM card tampering is found, including disassembling of the device, the warranty will be null and void.

Motorola is not responsible for any accessories, or device batteries, that are shipped with the device for repair.

Device software releases. The Customer will be responsible for updating each eligible BWC device with the latest available software and/or firmware, and of advising users of any operational changes that may have been introduced as a result of the new software or firmware.

LTE/4G Service. The Customer is responsible for selecting a Motorola approved LTE/4G Carrier/Provider during the initial ordering process, and for contacting the Carrier and activating LTE service for the device. The Customer is solely responsible for all financial obligations with the selected LTE Carrier.

Wi-Fi Connectivity. The Customer is responsible for providing all Wi-Fi connectivity to the device.

Removing Customer Data. The Customer is responsible for removing, from the device, any data, video, or other information that the Customer wishes to retain or destroy, prior to sending the device to a Motorola Repair Center for repair.

Motorola may provide a Video Evidence Recovery Service for the BWC device, as an additional charge. Video Evidence Recovery is a best effort service that is dependent on the condition of the device. This service, if applicable, will have a separated Agreement, with Terms and Conditions, outside the scope of this Statement of Work (SOW). Please contact your Motorola Representative for more information regarding the Video Evidence Recovery Service.

Essential Service Limitations and Restrictions

Customer will incur additional charges at the prevailing rates for any of the following activities, which are not covered under this Agreement:

- Replacement of consumable parts or accessories, as defined by product, including but not limited to batteries, cables, mounts, or clips.
- Repair of problems caused by natural or manmade disasters, including but not limited to fire, theft and floods that would cause internal or external component damage or destruction.
- Repair of problems caused by third parties' Software, accessories or peripherals not approved in writing by Motorola for use with the device.
- Repair of problems caused by using the device outside of the product's operational and environmental specifications, including improper handling, carelessness or reckless use, or repaired by a third party.
- Repair of problems caused by unauthorized alterations or attempted repair.
- Non-remedial work, including but not limited to administration and operator procedures, reprogramming, and operator or user training.
- Problem determination and/or work performed to repair or resolve issues with non-covered products; for example, any hardware or software products not specifically listed on the service order form.
- Any file or video backup or restoration.
- Completion and test of incomplete application programming or system integration if not performed by Motorola and specifically listed as covered.
- Use of Software or Firmware releases, except as provided for under the responsibilities outlined in this document.
- Accidental damage, chemical or liquid damage, or other damage caused outside of normal device operating specifications, unless the Customer has purchased the optional Essential Service with Accidental Damage and Advanced Replacement package.
- Cosmetic imperfections that do not affect the functionality of the device.

Where a Body Worn Camera device is submitted for repair that is outside the scope of Service, such repair may be quoted by Motorola for additional cost in accordance with Motorola's standard Time and Materials (T&M) rates and terms and conditions. Motorola will notify the Customer of any incremental charges related to the aforementioned exclusions prior to completing the repair and said repair will be subject to acceptance of the quotation by the Customer.

Software support for unauthorized modifications, or other misuse of the device software, is not covered under this Agreement.

Access to the software and firmware releases for updating the device under this SOW is available only for the device named in the Agreement. Software updates to any additional devices are expressly excluded and prohibited. Notwithstanding the foregoing, Motorola may, at its sole discretion, include coverage for other devices.

Any implementation tools not required to support the device software and firmware updates are excluded from coverage.

Motorola Solutions is not obligated to provide support for any Device:

- That has been repaired, tampered with, altered or modified (including the unauthorized installation of any software) — except by Motorola authorized service personnel.
- That has been subjected to unusual physical or electrical stress, abuse, or forces or exposure beyond normal use within the specified operational and environmental parameters set forth in the applicable product specification.
- If Customer fails to comply with the obligations contained in the product purchase agreement and/or the applicable software license agreement and/or Motorola terms and conditions of service.

1.10. Essential Service with Accidental Damage Repair and Advanced Replacement

Description of Services and Obligations

Accidental Damage coverage is an optional, prepaid service that adds coverage for accidentally damaged BWC devices. Accidental Damage coverage must be purchased together with, or within 90 days of, a qualifying Motorola device purchase. This three (3) or five (5) year service offer reduces unexpected expenses related to the repair of the device. Accidental Damage and Advanced Replacement coverage includes all services provided under Essential Service, plus additional coverage for Accidental Damage and Advanced Replacement of the damaged device.

Examples of repairs covered under Accidental Damage include:

- Electrical repair for failures caused by accidental water or chemical damage.
- Electrical repair for accidental internal damage.
- Replacement of accidentally cracked or broken housings.
- Replacement of accidentally cracked or broken camera lens or displays.
- Replacement of accidentally cracked or broken or missing buttons, knobs, or keypads.

Repair or Replacement. Motorola will provide repair or replacement of a BWC device, at its option, with a five (5) business day in-house turnaround time, excluding weekends and holidays, provided the device is delivered to the repair center by 9:00 a.m. (local repair center time), and replacement parts, components, and/or devices are available. Repair may include the replacement of parts, or boards with new parts or complete boards or, at Motorola option, with functionally equivalent, reconditioned parts, boards, or with a new replacement or refurbished device. All replaced parts, boards or devices will become the property of

Motorola. Turnaround time represents the time a product spends in the repair process; it does not include time in transit, including customs clearance.

Serial Numbers. If the Accidental Damage Service is purchased with the device, in the same order, using Motorola's Partner Hub Portal, OCC, or CPQ when ordering, the hardware serial number(s) are automatically captured and included in the Service Agreement. If Accidental Damage Service is purchased within 90 days of device shipment, the Customer must provide a complete list, preferably in electronic format, or by completing a Service Order Form (SOF), of all hardware serial numbers to be covered under the Agreement.

Initiating Repair. When initiating a repair, the Customer must contact Motorola to obtain a Return Material Authorization (RMA) number for each faulty BWC device. The Customer can submit a repair, and request an RMA, via the Partner Hub Portal, or by contacting the Motorola's Service Desk. If two-way shipping is included, the customer can generate a shipping label via Partner Hub, or by contacting the Motorola Service Desk. The Return Material Authorization (RMA) must be included with the device when shipped to the Authorized Motorola Repair Center.

- Only the BWC device should be returned for repair. The battery must be removed before shipping the device to a Motorola Repair Center.
- Device accessories should not be included when returning a device to a Motorola Repair Center for repair. Accessories include batteries, chargers or charging stations, cables, mounts, and clips.
- The SIM card must remain in the device, and intact, when the device is shipped to a Motorola Repair Center. If the SIM card is removed, or if any evidence of SIM card tampering is found, including disassembling of the device, the warranty will be null and void.

Motorola is not responsible for any accessories, or device batteries, that are shipped with the device for repair.

Advanced Replacement. Under Accidental Damage and Advanced Replacement Service, Motorola will provide Advanced Replacement for the damaged device. Motorola will ship a new or refurbished replacement device to the Customer within two (2) business days of receiving the Customer repair request, subject to availability of replacement devices. Business days do not include weekends or holidays.

The Customer must return the defective or damaged device to a Motorola Repair Center within 60 days after receiving the replacement device. Failure to return the damaged device to Motorola will result in an additional Customer charge for the replacement device.

When returning a device for Advanced Replacement, device accessories should not be included. Accessories include batteries, chargers or charging stations, cables, mounts, and clips.

Motorola is not responsible for any accessories that are shipped with the device.

1.11. Accidental Damage and Advanced Replacement Limitations and Restrictions

Customer will incur additional charges at the prevailing rates for any of the following activities, which are not covered under this Agreement:

- Replacement of consumable parts or accessories, as defined by product, including but not limited to batteries, chargers, charging stations, mounts, and clips.

- Repair of problems caused by natural or manmade disasters, including but not limited to fire, theft and floods that would cause internal or external component damage or destruction.
- Repair of problems caused by third parties' Software, accessories or peripherals not approved in writing by Motorola for use with the device.
- Repair of problems caused by using the device outside of the product's operational and environmental specifications, including improper handling, carelessness or reckless use, or repair by a third party.
- Repair of problems caused by unauthorized alterations or attempted repair.
- Non-remedial work, including but not limited to administration and operator procedures, reprogramming, and operator or user training.
- Problem determination and/or work performed to repair or resolve issues with non-covered products; for example, any hardware or software products not specifically listed on the service order form.
- Any file or video backup or restoration.
- Completion and test of incomplete application programming or system integration if not performed by Motorola and specifically listed as covered.
- Use of Software or Firmware releases except as provided for under the responsibilities outlined in this document.

There is a maximum limit of one (1) Body Worn Camera device repair, per contract year, for Essential Service with Accidental Damage and Advanced Replacement.

Where ongoing "Accidental Damage" repair is deemed by Motorola to be excessive, systemic, or the result of device mishandling, the Customer may be subject to an additional charge. Should the accidental damage continue unabated, the Customer will incur repair charges at Motorola's discretion and prevailing charges for devices deemed by Motorola to have been damaged through improper handling, carelessness or reckless use.

Warranty

1.12. Limited Warranty

Motorola warrants each body-worn camera system, part, and component it manufactures first sold to an end user to be free from defects in material and workmanship for a period of ONE-YEAR from the date of purchase. A defective component that is repaired or replaced under this limited warranty will be covered for the remainder of the original warranty period. Where defects in material or workmanship may occur, the following warranty terms and conditions apply:

Warrantor

This warranty is granted by Motorola Solutions, Inc., 415 E Exchange Parkway, Allen, TX 75002. Telephone: 1-800-MSI-HELP.

Parties to Whom Warranty is Intended

This warranty extends to the original end user of the equipment only and is not transferable. Any exceptions must be approved in writing from Motorola.

Parts and Components Covered

All parts and components and repair labor of the warranted unit manufactured and/or installed by Motorola are covered by this warranty, except those parts and components excluded below.

Parts and Components Not Covered

The Limited Warranty excludes normal wear-and-tear items such as frayed or broken cords, broken connectors, and scratched or broken displays. Motorola reserves the right to charge for damages resulting from abuse, improper installation, or extraordinary environmental damage (including damages caused by spilled liquids) to the unit during the warranty period at rates normally charged for repairing such units not covered under the Limited Warranty. In cases where potential charges would be incurred due to said damages, the agency submitting the system for repairs must be notified. Altered, damaged, or removed serial numbers results in voiding this Limited Warranty. If while under the warranty period, it is determined that the Motorola system was internally changed, modified, or repair attempted, the system warranty will become null and void.

Limited Liability

Motorola's liability is limited to the repair or replacement of components found to be defective by Motorola. Motorola will not be liable for any indirect, consequential, or incidental damages arising out of the use of or inability to use the system even if the unit proved to be defective. Motorola will not be responsible for any removal or re-installation cost of the unit or for damages caused by improper installation.

Remedy

If, within the duration of this warranty, a unit or component covered by this warranty is determined by Motorola to be defective in material or workmanship, Motorola shall replace any defective components. Replacement of a defective component(s) pursuant to this warranty shall be warranted for the remainder of the warranty period applicable to the system warranty period. Motorola will advance ship a replacement unit, or at the request of the customer, ask for the unit to be sent in for repair. In the case of an advance shipment replacement, Motorola will supply a return label with the advance unit, and the customer must return the defect within thirty days.

Shipping

When an advance replacement is sent out, the unit will ship via ground shipping, and Motorola will provide a prepaid shipping label to return any defective unit for end users in the continental United States. A serial number is required to be submitted with the request in order to receive an advance replacement unit. The customer will need to contact Motorola's Customer Service Department to request a return material authorization (RMA) number. Failure to return the unit within the thirty-day window will result in the customer being billed the full purchase price of the advance shipped unit.

If the customer requests the unit be sent in for repair, the end user will be responsible for any shipping charges to Motorola. Motorola will return ship the product to a customer within the continental United States by prepaid ground shipping only. Any expedited shipping costs are the responsibility of the end user.

Customers that are outside the continental United States will be responsible for all transportation costs both to and from Motorola's factory for warranty service, including without limitation to any export or import fees, duties, tariffs, or any other related fees that may be incurred during transportation. You may also obtain warranty service by contacting your local Motorola Authorized Service Center (ASC) for shipping instructions. A list of local ASCs may be obtained by contacting Motorola's Customer Service Department. Customers will be responsible for all transportation costs to and from the local ASC for warranty service.

Extended Warranty

Extended Warranties may be purchased directly from Motorola. Any and all extended warranties must be purchased prior to the expiration of any previous warranty. Failure to purchase an extended warranty prior to the expiration of the warranty period will require the covered unit to be physically inspected at the facility of the manufacturer and any repairs necessary to bring the unit back to full working order must be performed prior to the issuance of any new warranty. The customer will be responsible for the cost of the inspection (equal to one hour of labor) plus the standard costs associated with any required repairs.

1.13. Three-Year Warranty

Motorola warrants each body-worn camera system, part, and component it manufactures first sold to an end user to be free from defects in material and workmanship for a period of THREE YEARS from the date of purchase. A defective component that is repaired or replaced under this limited warranty will be covered for the remainder of the original warranty period. Where defects in material or workmanship may occur, the following warranty terms and conditions apply:

Warrantor

This warranty is granted by Motorola Solutions, Inc., 415 E Exchange Parkway, Allen, TX 75002. Telephone: 1-800-MSI-HELP.

Parties to Whom Warranty is Intended

This warranty extends to the original end user of the equipment only and is not transferable. Any exceptions must be approved in writing from Motorola.

Parts and Components Covered

All parts and components, including consumable items such as batteries, and repair labor of the warranted unit manufactured and/or installed by Motorola are covered by this warranty, except those parts and components excluded below.

Parts and Components Not Covered

The Limited Warranty excludes camera mounts and normal wear-and-tear items such as frayed or broken cords and scratched or broken displays. Motorola reserves the right to charge for damages resulting from abuse, improper use, or extraordinary environmental damage (such as submersion in liquid) to the unit during the warranty period at rates normally charged for repairing such units not covered under the Limited Warranty. In cases where potential charges would be incurred due to said damages, the agency submitting

the system for repairs MUST be notified. Altered, damaged, or removed serial numbers results in voiding this Limited Warranty. If while under the warranty period, it is determined that the Motorola system was internally changed, modified, or repair attempted, the system warranty will become null and void.

Limited Liability

Motorola's liability is limited to the repair or replacement of components found to be defective by Motorola. Motorola will not be liable for any indirect, consequential, or incidental damages arising out of the use of or inability to use the system even if the unit proved to be defective.

Remedy

If, within the duration of this warranty, a unit or component covered by this warranty is diagnosed by Motorola's Customer Service phone support and proves to be defective in material or workmanship, Motorola shall replace the defective unit with an Advance Replacement unit. The Advance Replacement unit will ship via UPS ground and include a prepaid shipping label to return the defective unit, which must be received by Motorola within thirty days. The Advance Replacement unit pursuant to this warranty shall be warranted for the remainder of the warranty period.

Shipping

When an advance replacement is sent out, the unit will ship via ground shipping, and Motorola will provide a prepaid shipping label to return any defective unit for end users in the continental United States. A serial number is required to be submitted with the request in order to receive an advance replacement unit. The customer will need to contact Motorola's Customer Service Department to request a return material authorization (RMA) number. Failure to return the unit within the thirty-day window will result in the customer being billed the full purchase price of the advance shipped unit.

If the customer requests the unit be sent in for repair, the end user will be responsible for any shipping charges to Motorola. Motorola will return ship the product to a customer within the continental United States by prepaid ground shipping only. Any expedited shipping costs are the responsibility of the end user.

Customers outside the continental United States will be responsible for all transportation costs both to and from Motorola's factory for warranty service, including without limitation any export or import fees, duties, tariffs, or any other related fees that may be incurred during transportation. You may also obtain warranty service by contacting your local Motorola Authorized Service Center (ASC) for shipping instructions. A list of local ASCs may be obtained by contacting Motorola's Customer Service Department. Customers will be responsible for all transportation costs to and from the local ASC for warranty service.

Extended Warranty

A Five-Year Extended "No-Fault" Warranty may be purchased directly from Motorola. Any and all extended warranties must be purchased prior to the expiration of any previous warranty. Failure to purchase an extended warranty prior to the expiration of the warranty period will require the covered unit to be physically inspected at the facility of the manufacturer and any repairs necessary to bring the unit back to full working order must be performed prior to the issuance of any new warranty. The customer will be responsible for the cost of the inspection (equal to one hour of labor) plus the standard costs associated with any required repairs.

1.14. Five-Year Warranty

Motorola warrants each body-worn camera system, part, and component it manufactures first sold to an end user to be free from defects in material and workmanship for a period of five years from the date of purchase. A defective component that is repaired or replaced under this limited warranty will be covered for the remainder of the original warranty period. Where defects in material or workmanship may occur, the following warranty terms and conditions apply:

Warrantor

This warranty is granted by Motorola Solutions, Inc., 415 E Exchange Parkway, Allen, TX 75002. Telephone: 1-800-MSI-HELP.

Parties to Whom Warranty Is Intended

This warranty extends to the original end user of the equipment only and is not transferable. Any exceptions must be approved in writing from Motorola.

Parts and Components Covered

All parts and components, including consumable items such as batteries, and repair labor of the warranted unit manufactured and/or installed by Motorola are covered by this warranty, except those parts and components excluded below.

Parts and Components Not Covered

The Limited Warranty excludes camera mounts and normal wear-and-tear items such as frayed or broken cords and scratched or broken displays. Motorola reserves the right to charge for damages resulting from abuse, improper use, or extraordinary environmental damage (such as submersion in liquid) to the unit during the warranty period at rates normally charged for repairing such units not covered under the Limited Warranty. In cases where potential charges would be incurred due to said damages, the agency submitting the system for repairs MUST be notified. Altered, damaged, or removed serial numbers results in voiding this Limited Warranty. If while under the warranty period, it is determined that the Motorola system was internally changed, modified, or repair attempted, the system warranty will become null and void.

Limited Liability

Motorola's liability is limited to the repair or replacement of components found to be defective by Motorola. Motorola will not be liable for any indirect, consequential, or incidental damages arising out of the use of or inability to use the system even if the unit proved to be defective.

Remedy

If, within the duration of this warranty, a unit or component covered by this warranty is diagnosed by Motorola's Customer Service phone support and proves to be defective in material or workmanship, Motorola shall replace the defective unit with an Advance Replacement unit. The Advance Replacement unit will ship via UPS ground and include a prepaid shipping label to return the defective unit, which must be received by Motorola within thirty days. The Advance Replacement unit pursuant to this warranty shall be warranted for the remainder of the warranty period.

Shipping

When an advance replacement is sent out, the unit will ship via ground shipping, and Motorola will provide a prepaid shipping label to return any defective unit for end users in the continental United States. A serial number is required to be submitted with the request in order to receive an advance replacement unit. The customer will need to contact Motorola’s Customer Service Department to request a return material authorization (RMA) number. Failure to return the unit within the thirty-day window will result in the customer being billed the full purchase price of the advance shipped unit.

If the customer requests the unit be sent in for repair, the end user will be responsible for any shipping charges to Motorola. Motorola will return ship the product to a customer within the continental United States by prepaid ground shipping only. Any expedited shipping costs are the responsibility of the end user.

Customers that are outside the continental United States will be responsible for all transportation costs both to and from Motorola’s factory for warranty service, including without limitation any export or import fees, duties, tariffs, or any other related fees that may be incurred during transportation. You may also obtain warranty service by contacting your local Motorola Authorized Service Center (ASC) for shipping instructions. A list of local ASCs may be obtained by contacting Motorola’s Customer Service Department. Customers will be responsible for all transportation costs to and from the local ASC for warranty service.

- Include if quoting V700 Essential Services.
- Include if quoting V700 Essential Services with Accidental Damage Repair and Advanced Replacement.
- Include if quoting Premier Services.
- Standard Warranty that comes with all devices.
- Include if not quoting extended warranty for 3 or 5 years.
- Include if quoting 3 years extended warranty.
- Include if quoting 5-year extended warranty.

V700 Body Worn Camera “As-a Service” Warranty

High Level Warranty Replacement Term Length	
Body-Worn Camera	Every 3 years
Body-Worn Camera Battery	Every 1 to 2 years (dependent on use)
Body Worn Camera Mounts	As needed
In-Car Video system, part, and component	Every 3 to 5 years

Body Worn Camera

The Video-as-a-Service package includes our comprehensive No-Fault Warranty. Motorola warrants each system, part, and component we manufacturer first sold to an end user to be free of defects in materials and workmanship for one year (12-month period) from the date purchase in its Limited Warranty. The V300 comes with a standard one-year warranty with an option to extend the warranty. Our price proposal includes pricing for extended warranty coverage through the fifth year of system ownership. Body worn

cameras come with a three-year warranty and a refresh program at the end of the third year, where old units will be replaced with new body worn cameras. Body worn cameras camera refreshes are warranted until the end of the 5th year contract.

Motorola's Video-as-a-Service package (VaaS) includes a "no fault" hardware warranty for the duration of the contract and a body-worn camera hardware refresh in the third year. Motorola has the industry's most flexible warranty program, and no fault literally means "no fault." Cameras can be crushed or smashed, frozen or melted. We will send you a replacement. Please see the attached VaaS Video as a Service Addendum that details the No-Fault Warranty.

No-Fault Warranty. Subject to the disclaimers set forth in the MCA and EPSLA, upon delivery of any Equipment purchased as part of the VaaS Program, Motorola will provide a No-fault Warranty to Customer for such Equipment that extends until the end of the Commitment Term (as defined below) applicable to such Equipment; except that the No-fault Warranty will not apply to (i) any Equipment with intentionally altered or removed serial numbers, (ii) any other damages disclaimed under the MCA or EPSLA, or (iii) any Equipment that Motorola determines was changed, modified, or repaired by Customer or any third party. The "No-fault Warranty" means that Motorola will repair or replace any Equipment components or parts that render the applicable Equipment unable to perform its intended purpose. With respect to any batteries in body-worn cameras, a battery will be considered faulty and covered under this No-fault Warranty if it falls below sixty percent (60%) of rated capacity.

An "advance replacement" warranty is also included. Should a unit need to be sent in for repair, Customer will call support and open a ticket. A replacement unit will be sent out within 48 hours of the ticket being opened.

Advance replacement equipment will be shipped within 24 hours of notification.

In-Car Camera Warranty

In car video warranties cover the duration of the contract, and additional sixth- or seventh-year warranties can be purchased as needed.

Motorola warrants each camera system, part, and component it manufactures first sold to an end user to be free from defects in material and workmanship for a period of five years from the date of purchase. A defective component that is repaired or replaced under this limited warranty will be covered for the remainder of the original warranty period. Where defects in material or workmanship may occur, the following warranty terms and conditions apply:

Warrantor

This warranty is granted by Motorola Solutions, Inc., 415 E Exchange Parkway, Allen, TX 75002. Telephone: 1-800-MSI-HELP.

Parties to Whom Warranty Is Intended

This warranty extends to the original end user of the equipment only and is not transferable. Any exceptions must be approved in writing from Motorola.

Parts and Components Covered

All parts and components, including consumable items such as batteries, and repair labor of the warranted unit manufactured and/or installed by Motorola are covered by this warranty, except those parts and components excluded below.

Parts and Components Not Covered

The Limited Warranty excludes camera mounts and normal wear-and-tear items such as frayed or broken cords and scratched or broken displays. Motorola reserves the right to charge for damages resulting from abuse, improper use, or extraordinary environmental damage (such as submersion in liquid) to the unit during the warranty period at rates normally charged for repairing such units not covered under the Limited Warranty. In cases where potential charges would be incurred due to said damages, the agency submitting the system for repairs MUST be notified. Altered, damaged, or removed serial numbers results in voiding this Limited Warranty. If while under the warranty period, it is determined that the Motorola system was internally changed, modified, or repair attempted, the system warranty will become null and void.

Limited Liability

Motorola's liability is limited to the repair or replacement of components found to be defective by Motorola. Motorola will not be liable for any indirect, consequential, or incidental damages arising out of the use of or inability to use the system even if the unit proved to be defective.

Remedy

If, within the duration of this warranty, a unit or component covered by this warranty is diagnosed by Motorola's Customer Service phone support and proves to be defective in material or workmanship, Motorola shall replace the defective unit with an Advance Replacement unit. The Advance Replacement unit will ship via UPS ground and include a prepaid shipping label to return the defective unit, which must be received by Motorola within thirty days. The Advance Replacement unit pursuant to this warranty shall be warranted for the remainder of the warranty period.

Shipping

When an advance replacement is sent out, the unit will ship via ground shipping, and Motorola will provide a prepaid shipping label to return any defective unit for end users in the continental United States. A serial number is required to be submitted with the request in order to receive an advance replacement unit. The customer will need to contact Motorola's Customer Service Department to request a return material authorization (RMA) number. Failure to return the unit within the thirty-day window will result in the customer being billed the full purchase price of the advance shipped unit.

If the customer requests the unit be sent in for repair, the end user will be responsible for any shipping charges to Motorola. Motorola will return ship the product to a customer within the continental United States by prepaid ground shipping only. Any expedited shipping costs are the responsibility of the end user.

Customers that are outside the continental United States will be responsible for all transportation costs both to and from Motorola's factory for warranty service, including without limitation any export or import fees, duties, tariffs, or any other related fees that may be incurred during transportation. You may also obtain warranty service by contacting your local Motorola Authorized Service Center (ASC) for shipping instructions. A list of local ASCs may be obtained by contacting Motorola's Customer Service Department. Customers will be responsible for all transportation costs to and from the local ASC for warranty service.

SCHEDULE O - SERVICE LEVEL AGREEMENT FOR HYBRID PURCHASES

1. **Definitions.** For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Schedule** shall have the respective meanings given to them in the Contract Terms and Conditions.

“**Actual Uptime**” means the total minutes in the Service Period that the Hosted Services are Available.

“**Availability**” has the meaning set forth in **Section 2.1**.

“**Availability Requirement**” has the meaning set forth in **Section 2.1**.

“**Available**” has the meaning set forth in **Section 2.1**.

“**Contact List**” means a current list of Contractor contacts and telephone numbers set forth in the attached **Schedule D – Attachment 1** to this Schedule to enable the State to escalate its Support Requests, including: (a) the first person to contact; and (b) the persons in successively more qualified or experienced positions to provide the support sought.

“**Corrective Action Plan**” has the meaning set forth in **Section 3.9**.

“**Critical Service Error**” has the meaning set forth in **Section 3.5**.

“**Exceptions**” has the meaning set forth in **Section 2.2**.

“**High Service Error**” has the meaning set forth in **Section 3.5**.

“**Hosted Services**” means the hosting, management and operation of the Operating Environment, Software, other services (including support and subcontracted services), and related resources for remote electronic access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

“**Low Service Error**” has the meaning set forth in **Section 3.5**.

“**Maintenance Release**” means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide to its licensees from time to time during the Term, which may contain, among other things, error corrections, enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

“**Medium Service Error**” has the meaning set forth in **Section 3.5**.

“**New Version**” means any new version of the Software, including any updated Documentation, that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

“**Operating Environment**” means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in a Statement of Work,

including such structural, functional and other features, conditions and components as hardware, operating software, system architecture, configuration, computing hardware, ancillary equipment, networking, software, firmware, databases, data, and electronic systems (including database management systems).

“**Resolve**” has the meaning set forth in **Section 3.6**.

“**RPO**” or “**Recovery Point Objective**” means the maximum amount of potential data loss in the event of a disaster.

“**RTO**” or “**Recovery Time Objective**” means the maximum period of time to fully restore the Hosted Services in the case of a disaster.

“**Scheduled Downtime**” has the meaning set forth in **Section 2.3**.

“**Scheduled Uptime**” means the total minutes in the Service Period.

“**Service Availability Credits**” has the meaning set forth in **Section 2.6(a)**.

“**Service Error**” means any failure of any Hosted Service to be Available or otherwise perform in accordance with this Schedule.

“**Service Level Credits**” has the meaning set forth in **Section 3.8**.

“**Service Level Failure**” means a failure to perform the Software Support Services fully in compliance with the Support Service Level Requirements.

“**Service Period**” has the meaning set forth in **Section 2.1**.

“**Software Support Services**” has the meaning set forth in **Section 3**.

“**State Systems**” means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

“**Support Hours**” means the contracted hours when the service is supported during normal business hours.

“**Support Request**” has the meaning set forth in **Section 3.5**.

“**Support Service Level Requirements**” has the meaning set forth in **Section 3.4**.

2. Service Availability and Service Availability Credits.

2.1. Availability Requirement. Contractor will make the Hosted Services and Software Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Hosted Services (each such calendar month, a “**Service Period**”), at least 99.98% of the time, excluding only the time the Hosted Services are not Available solely as a result of one or more Exceptions (the “**Availability Requirement**”). “**Available**” means the Hosted Services and Software are available and operable for access and use by the State and its Authorized Users over the Internet in material conformity with the Contract. “**Availability**” has a correlative meaning. The Hosted Services and Software are not considered Available in the event of a material performance degradation or inoperability of the

Hosted Services and Software, in whole or in part. The Availability Requirement will be calculated for the Service Period as follows: $(\text{Actual Uptime} - \text{Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception}) \div (\text{Scheduled Uptime} - \text{Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception}) \times 100 = \text{Availability}$.

2.2. Exceptions. No period of Hosted Services degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to any of the following (“**Exceptions**”):

- a) Failures of the State’s or its Authorized Users’ internet connectivity;
- b) Scheduled Downtime as set forth in **Section 2.3**.

2.3 Scheduled Downtime. Contractor must notify the State at least twenty-four (24) hours in advance of all scheduled outages of the Hosted Services or Software in whole or in part (“**Scheduled Downtime**”). All such scheduled outages will: (a) last no longer than five (5) hours; (b) be scheduled between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time; and (c) occur no more frequently than once per week; provided that Contractor may request the State to approve extensions of Scheduled Downtime above five (5) hours, and such approval by the State may not be unreasonably withheld or delayed.

2.4 Software Response Time. Software response time, defined as the interval from the time the end user sends a transaction to the time a visual confirmation of transaction completion is received, must be less than two (2) seconds for 98% of all transactions. Unacceptable response times shall be considered to make the Software unavailable and will count against the Availability Requirement.

2.5 Service Availability Reports. Within thirty (30) days after the end of each Service Period, Contractor will provide to the State a report describing the Availability and other performance of the Hosted Services and Software during that calendar month as compared to the Availability Requirement. The report must be in electronic or such other form as the State may approve in writing and shall include, at a minimum: (a) the actual performance of the Hosted Services and Software relative to the Availability Requirement; and (b) if Hosted Service performance has failed in any respect to meet or exceed the Availability Requirement during the reporting period, a description in sufficient detail to inform the State of the cause of such failure and the corrective actions the Contractor has taken and will take to ensure that the Availability Requirement are fully met.

2.6 Remedies for Service Availability Failures.

- a) If the actual Availability of the Hosted Services and Software is less than the Availability Requirement for any Service Period, such failure will constitute a Service Error for which Contractor will issue to the State the following credits on the fees payable for Hosted Services and Software provided during the Service Period (“**Service Availability Credits**”):

Availability	Credit of Fees
≥99.98%	None

Availability	Credit of Fees
<99.98% but ≥99.0%	15%
<99.0% but ≥95.0%	50%
<95.0%	100%

- b) Any Service Availability Credits due under this **Section** will be applied in accordance with payment terms of the Contract.
- c) If the actual Availability of the Hosted Services and Software is less than the Availability Requirement in any two (2) of four (4) consecutive Service Periods, then, in addition to all other remedies available to the State, the State may terminate the Contract on written notice to Contractor with no liability, obligation or penalty to the State by reason of such termination.

3. Support and Maintenance Services. Contractor will provide IT Environment Service and Software maintenance and support services (collectively, “**Software Support Services**”) in accordance with the provisions of this **Section 3**. The Software Support Services are included in the Services, and Contractor may not assess any additional fees, costs or charges for such Software Support Services.

3.1 Support Service Responsibilities. Contractor will:

- a) correct all Service Errors in accordance with the Support Service Level Requirements, including by providing defect repair, programming corrections and remedial programming;
- b) provide unlimited telephone support during **Support Hours**;
- c) provide unlimited online support 24 hours a day, seven days a week;
- d) provide online access to technical support bulletins and other user support information and forums, to the full extent Contractor makes such resources available to its other customers; and
- e) respond to and Resolve Support Requests as specified in this **Section**.

3.2 Service Monitoring and Management. Contractor will continuously monitor and manage the Hosted Services and Software to optimize Availability that meets or exceeds the Availability Requirement. Such monitoring and management includes:

- a) proactively monitoring on a twenty-four (24) hour by seven (7) day basis all Hosted Service functions, servers, firewall and other components of Hosted Service security;
- b) if such monitoring identifies, or Contractor otherwise becomes aware of, any circumstance that is reasonably likely to threaten the Availability of the Hosted Service, taking all necessary and reasonable remedial measures to promptly eliminate such threat and ensure full Availability; and
- c) if Contractor receives knowledge that the Hosted Service or any Hosted Service function or component is not Available (including by written notice from the State pursuant to the procedures set forth herein):

- (i) confirming (or disconfirming) the outage by a direct check of the associated facility or facilities;
- (ii) If Contractor's facility check in accordance with clause (i) above confirms a Hosted Service outage in whole or in part: (A) notifying the State in writing pursuant to the procedures set forth herein that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Section 3.5** and **3.6**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and
- (iii) Notifying the State that Contractor has fully corrected the outage and any related problems, along with any pertinent findings or action taken to close the trouble ticket.

3.3 Service Maintenance. Contractor will continuously maintain the Hosted Services and Software to optimize Availability that meets or exceeds the Availability Requirement. Such maintenance services include providing to the State and its Authorized Users:

- a) all updates, bug fixes, enhancements, Maintenance Releases, New Versions and other improvements to the Hosted Services and Software, including the Software, that Contractor provides at no additional charge to its other similarly situated customers; provided that Contractor shall consult with the State and is required to receive State approval prior to modifying or upgrading Hosted Services and Software, including Maintenance Releases and New Versions of Software; and
- b) all such services and repairs as are required to maintain the Hosted Services and Software or are ancillary, necessary or otherwise related to the State's or its Authorized Users' access to or use of the Hosted Services and Software, so that the Hosted Services and Software operate properly in accordance with the Contract and this Schedule.

3.4 Support Service Level Requirements. Contractor will correct all Service Errors and respond to and Resolve all Support Requests in accordance with the required times and other terms and conditions set forth in this **Section 3.4 ("Support Service Level Requirements")**, and the Contract.

3.5 Support Requests. The State will classify its requests for Service Error corrections in accordance with the descriptions set forth in the chart below (each a "**Support Request**"). The State will notify Contractor of Support Requests by email, telephone or such other means as the parties may hereafter agree to in writing.

Support Request Classification	Description: Any Service Error Comprising or Causing any of the Following Events or Effects
Critical Service Error	<ul style="list-style-type: none"> • Issue affecting entire system or single critical production function; • System down or operating in materially degraded state; • Data integrity at risk; • Declared a Critical Support Request by the State; or • Widespread access interruptions.
High Service Error	<ul style="list-style-type: none"> • Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis.
Medium Service Error	<ul style="list-style-type: none"> • IT Environment Services and Software is operating with minor issues that can be addressed with an acceptable (as determined by the State) temporary work around.
Low Service Error	<ul style="list-style-type: none"> • Request for assistance, information, or services that are routine in nature.

3.6 Response and Resolution Time Service Levels. Response and Resolution times will be measured from the time Contractor receives a Support Request until the respective times Contractor has (i) responded to, in the case of response time and (ii) Resolved such Support Request, in the case of Resolution time. **“Resolve”** (including **“Resolved”**, **“Resolution”** and correlative capitalized terms) means that, as to any Service Error, Contractor has provided the State the corresponding Service Error correction and the State has confirmed such correction and its acceptance thereof. Contractor will respond to and Resolve all Service Errors within the following times based on the severity of the Service Error:

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
Critical Service Error	One (1) hour	Three (3) hours	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.
High Service Error	One (1) hour	Four (4) hours	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.
Medium Service Error	Three (3) hours	Two (2) Business Days	N/A	N/A
Low Service Error	Three (3) hours	Five (5) Business Days	N/A	N/A

3.7 Escalation. With respect to any Critical Service Error Support Request, until such Support Request is Resolved, Contractor will escalate that Support Request within sixty (60) minutes of the receipt of such Support Request by the appropriate Contractor support personnel, including, as applicable, the Contractor Project Manager and Contractor's management or engineering personnel, as appropriate.

3.8 Support Service Level Credits. Failure to achieve any of the Support Service Level Requirements for Critical and High Service Errors will constitute a Service Level Failure for which Contractor will issue to the State the corresponding service credits set forth in **Section 3.6 ("Service Level Credits")** in accordance with payment terms set forth in the Contract.

3.9 Corrective Action Plan. If two or more Critical Service Errors occur in any thirty (30) day period during (a) the Term or (b) any additional periods during which Contractor does or is required to perform any Hosted Services, Contractor will promptly investigate the root causes of these Service Errors and provide to the State within five (5) Business Days of its receipt of notice of the second such Support Request an analysis of such root causes and a proposed written corrective action plan for the State's review, comment and approval, which, subject to and upon the State's written approval, shall be a part of, and by this reference is incorporated in, the Contract as the parties' corrective action plan (the "**Corrective Action Plan**"). The Corrective Action Plan must include, at a minimum: (a) Contractor's commitment to the State to devote the appropriate time, skilled personnel, systems support and equipment and other resources necessary to Resolve and prevent any further occurrences of the Service Errors giving rise to such Support Requests; (b) a strategy for developing any programming, software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, such Service Errors; and (c) time frames for implementing the Corrective Action Plan. There will be no additional charge for Contractor's preparation or implementation of the Corrective Action Plan in the time frames and manner set forth therein.

4. Data Storage, Backup, Restoration and Disaster Recovery. Contractor must maintain or cause to be maintained backup redundancy and disaster avoidance and recovery procedures designed to safeguard State Data and the State's other Confidential Information, Contractor's Processing capability and the availability of the IT Environment Services and Software, in each case throughout the Term and at all times in connection with its actual or required performance of the Services hereunder. All backed up State Data shall be located in the continental United States. The force majeure provisions of this Contract do not limit Contractor's obligations under this section.

4.2 Data Storage. Contractor will provide sufficient storage capacity to meet the needs of the State at no additional cost.

4.3 Data Backup. Contractor will conduct, or cause to be conducted, daily back-ups of State Data and perform, or cause to be performed, other periodic offline back-ups of State Data on at least a weekly basis and store and retain such back-ups as specified in **Schedule A**. Contractor must, within five (5) Business Days of the State's request, provide the State, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor), an extract of State Data in the format specified by the State.

- 4.4 Data Restoration.** If the data restoration is required due to the actions or inactions of the Contractor or its subcontractors, Contractor will promptly notify the State and complete actions required to restore service to normal production operation. If requested, Contractor will restore data from a backup upon written notice from the State. Contractor will restore the data within one (1) Business Day of the State's request. Contractor will provide data restorations at its sole cost and expense.
- 4.5 Disaster Recovery.** Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and operate a backup and disaster recovery plan to achieve a Recovery Point Objective (RPO) of 4 hours, and a Recovery Time Objective (RTO) of 8-24 hours (the "**DR Plan**"), and implement such DR Plan in the event of any unplanned interruption of the Hosted Services. Contractor's current DR Plan, revision history, and any reports or summaries relating to past testing of or pursuant to the DR Plan are included or attached as described in **Schedule A** under **Hosting**. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance. Contractor will provide the State with copies of all such updates to the Plan within fifteen (15) days of its adoption by Contractor. All updates to the DR Plan are subject to the requirements of this **Section 3**; and provide the State with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor's receipt or preparation. If Contractor fails to reinstate all material Hosted Services and Software within the periods of time set forth in the DR Plan, the State may, in addition to any other remedies available under this Contract, in its sole discretion, immediately terminate this Contract as a non-curable default.

SCHEDULE P - DATA SECURITY REQUIREMENTS FOR HYBRID PURCHASES

1. **Definitions.** For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Schedule** shall have the respective meanings given to them in the Contract.

“**Contractor Security Officer**” has the meaning set forth in **Section 2** of this Schedule.

“**FedRAMP**” means the Federal Risk and Authorization Management Program, which is a federally approved risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

“**FISMA**” means The Federal Information Security Modernization Act of 2014 (Pub.L. No. 113-283 (Dec. 18, 2014.)).

“**Hosting Provider**” means any subcontractor that is providing any or all of the Hosted Services under this Contract.

“**Hosted Services**” means the hosting, management and operation of the Operating Environment, Software, other services (including support and subcontracted services), and related resources for remote electronic access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

“**NIST**” means the National Institute of Standards and Technology.

“**Operating Environment**” means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in a Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software, system architecture, configuration, computing hardware, ancillary equipment, networking, software, firmware, databases, data, and electronic systems (including database management systems).

“**PCI**” means the Payment Card Industry.

“**Process**” means to perform any operation or set of operations on any data, information, material, work, expression or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or (c) block, erase or destroy. “**Processing**” and “**Processed**” have correlative meanings.

“**PSP**” or “**PSPs**” means the State’s IT Policies, Standards and Procedures.

“**SSAE**” means Statement on Standards for Attestation Engagements.

“**Security Accreditation Process**” has the meaning set forth in **Section 6** of this Schedule

2. **Security Officer.** Contractor will appoint a Contractor employee to respond to the State's inquiries regarding the security of the Hosted Services who has sufficient knowledge of the security of the Hosted Services and the authority to act on behalf of Contractor in matters pertaining thereto ("**Contractor Security Officer**").
3. **Contractor Responsibilities.** Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to:
 - a) ensure the security and confidentiality of the State Data;
 - b) protect against any anticipated threats or hazards to the security or integrity of the State Data;
 - c) protect against unauthorized disclosure, access to, or use of the State Data;
 - d) ensure the proper disposal of any State Data in Contractor's or its subcontractor's possession; and
 - e) ensure that all Contractor Representatives comply with the foregoing.

The State has established Information Technology (IT) PSPs to protect IT resources under the authority outlined in the overarching State 1305.00 Enterprise IT Policy. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must at all times comply with all applicable public and non-public State IT policies and standards, of which the publicly available ones are at [DTMB - IT Policies, Standards & Procedures \(michigan.gov\)](#), to the extent those policies and standards align to the NIST 800-53 moderate security baseline and the organization defined parameters and control enhancements when articulated by the FBI in connection with its current version of the CJIS Security Policy.

This responsibility also extends to all service providers and subcontractors with access to State Data or an ability to impact the contracted solution. Contractor responsibilities are determined from the PSPs based on the services being provided to the State, the type of IT solution, and the applicable laws and regulations.

4. **Acceptable Use Policy.** To the extent that Contractor has access to the State's IT environment, Contractor must comply with the State's Acceptable Use Policy, see [1340.00.130.02 Acceptable Use of Information Technology \(michigan.gov\)](#). All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing State systems. The State reserves the right to terminate Contractor's and/or subcontractor(s) or any Contractor Personnel's access to State systems if the State determines a violation has occurred.
5. **Protection of State's Information.** Throughout the Term and at all times in connection with its actual or required performance of the Contract Activities, Contractor will:
 - 5.1 If Hosted Services are provided by a Hosting Provider, ensure each Hosting Provider maintains FedRAMP authorization for all Hosted Services environments throughout the Term, and in the event a Hosting Provider is unable to maintain FedRAMP authorization, the State, at its sole discretion,

may either a) require the Contractor to move the Software and State Data to an alternative Hosting Provider selected and approved by the State at Contractor's sole cost and expense without any increase in Fees, or b) immediately terminate this Contract for cause pursuant to **Section 25** of the Contract;

- 5.2** for Hosted Services provided by the Contractor, maintain either a FedRAMP authorization or an annual SSAE 18 SOC 2 Type II audit based on State required NIST Special Publication 800-53 MOD Controls or SOC 2 Type II trust criteria. Further, Contractor acknowledges and understands that the State may conduct its own Security Accreditation Process (as described in section 6 below) that may evaluate Contractor provided Hosted Services to NIST 800-53 MOD Controls.
- 5.3** ensure that the Software and State Data is securely stored, hosted, supported, administered, accessed, developed, and backed up in the continental United States, and the data center(s) in which the data resides minimally meet Uptime Institute Tier 3 standards (www.uptimeinstitute.com), or its equivalent;
- 5.4** maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State Data that complies with the requirements of the State's data security policies as set forth in this Contract, and must, at a minimum, remain compliant with FISMA and NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs;
- 5.5** provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, encryption, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of State Data and the nature of such State Data, consistent with best industry practice and applicable standards (including, but not limited to, compliance with FISMA, NIST, CMS, IRS, FBI, SSA, HIPAA, FERPA and PCI requirements as applicable);
- 5.6** take all reasonable measures to:
 - a) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Contract Activities that are within its control and ensure its subcontractors do the same against "malicious actors" and others who may seek, without authorization, to destroy, disrupt, damage, encrypt, modify, copy, access or otherwise use Hosted Services or the information found therein; and
 - b) prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Contract Activities; (ii) State Data from being commingled with or contaminated by the data of other customers or their users of the Contract Activities; and (iii) unauthorized access to any of the State Data;
- 5.7** ensure that State Data is encrypted in transit and at rest using FIPS validated AES encryption modules and a key size of 128 bits or higher;

- 5.8** ensure the Hosted Services support Identity Federation/Single Sign-on (SSO) capabilities using Security Assertion Markup Language (SAML), Open Authentication (OAuth) or comparable State approved mechanisms;
- 5.9** ensure the Hosted Services implements NIST compliant multi-factor authentication for privileged/administrative and other identified access.
- 6. Security Accreditation Process.** Throughout the Term, Contractor will assist the State, at no additional cost, with its **Security Accreditation Process**, which includes the development, completion and on-going maintenance of a system security plan (SSP) using the State's automated governance, risk and compliance (GRC) platform, which requires Contractor to submit evidence, upon request from the State, in order to validate Contractor's security controls within thirty (30) days of the State's request. On an annual basis, or as otherwise required by the State such as for significant changes, re-assessment of the system's controls will be required to receive and maintain authority to operate (ATO). All identified risks from the SSP will be remediated through a Plan of Action and Milestones (POAM) process with remediation time frames and required evidence based on the risk level of the identified risk. For all findings associated with the Contractor's solution, at no additional cost, Contractor will be required to participate in negotiations around the creation of State approved POAMs, perform related remediation activities within mutually agreeable timeframes if not otherwise dictated by applicable standards or FBI CJIS Policy, and provide evidence of compliance. For clarity, the State makes all decisions on the level of risk it is willing to accept.
- 7. Unauthorized Access.** Contractor may not access, and must not permit any access to, State systems, in whole or in part, whether through the Hosted Services or otherwise, without the State's express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Any access to State systems must be solely in accordance with the Contract and this Schedule, and in no case exceed the scope of the State's authorization pursuant to this Section. All State-authorized connectivity or attempted connectivity to State systems shall be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in the Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.
- 8. Security Audits.**
- 8.1** During the Term, Contractor will maintain complete and accurate records of its data protection practices, IT security controls, and the security logs relating to State Data, including but not limited to any backup, disaster recovery or other policies, practices or procedures relating to the State Data and any other information relevant to its compliance with this Contract.
- 8.2** Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program relevant to the scope of the products and services purchased prior to the commencement of Contract Activities and no more than annually thereafter during the term of this Contract. Such review will be conducted through information security and privacy questionnaires for Contractor's response as well as Contractor providing its related SOC 2

Type II report. The State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program relevant to the products and services purchased hereunder. No audit may be performed within a data center for security reasons. If the State chooses to perform an on-site audit, Contractor will, make all such records, appropriate personnel and relevant materials available during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least thirty (30) Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; and (iii) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Contract.

8.3 During the Term, Contractor will, when requested by the State, provide a copy of Contractor's and Hosting Provider's FedRAMP System Security Plan(s) or SOC 2 Type II report(s) to the State within two weeks of the State's request. The System Security Plan and SSAE audit reports will be recognized as Contractor's Confidential Information.

8.4 The State reserves the right, at its sole election, to immediately terminate this Contract or a Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this **Section 8**.

9. Application Scanning. During the Term, Contractor must, at its sole cost and expense, no less than monthly scan all Contractor provided applications, and must analyze, remediate and validate all vulnerabilities identified by the scans for existing code and for new code prior to deployment or as required by the CJIS Security Policy based on CVE Score.

Contractor's application scanning and remediation must include each of the following types of scans and activities:

9.1 Dynamic Application Security Testing (DAST) – Scanning interactive application for vulnerabilities, analysis, remediation, and validation (may include Interactive Application Security Testing (IAST)).

a) Contractor may dynamically scan a deployed version of the Software using a commercially reasonable application scanning tool, and no less than semi-annually provide the State with the number of vulnerabilities discovered and mitigated by severity.

9.2 Static Application Security Testing (SAST) - Scanning source code for vulnerabilities, analysis, remediation, and validation.

a) For Contractor provided applications, Contractor, at its sole expense, may provide resources to complete static application source code scanning, including the analysis, remediation and validation of vulnerabilities identified by application source code scans. Contractor will also

no less than semi-annually provide the State with the number of vulnerabilities discovered and mitigated per code release.

9.3 Software Composition Analysis (SCA) – Third Party and/or Open Source Scanning for vulnerabilities, analysis, remediation, and validation.

- a) For Software that includes third party and open source software, all included third party and open source software must be documented and the source supplier must be monitored by the Contractor for notification of identified vulnerabilities and remediation. SCA scans may be included as part of SAST and DAST scanning or employ the use of an SCA tool to meet the scanning requirements. Contractor will also no less than semi-annually provide the State with the number of vulnerabilities discovered and mitigated by software component.

9.4 In addition, application scanning and remediation may include the following types of scans and activities if required by regulatory or industry requirements, data classification or otherwise identified by the State.

- a) If provided as part of the solution, all native mobile application software must meet these scanning requirements including any interaction with an application programming interface (API).
- b) Penetration Testing – Simulated attack on the application and infrastructure to identify security weaknesses.

10. Infrastructure Scanning.

10.1 For Hosted Services, Contractor must monitor and scan for vulnerabilities in the infrastructure which is within Contractor's control, system, and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported; using a mutually agreed upon industry standard scanning tool, provide a scan summary which includes number of vulnerabilities by severity and monthly age for each of 30, 60, 90, and older than 90 days. Contractor will ensure the remediation of issues identified in the scan according to the remediation time requirements documented in the CJIS Security Policy.

11. Nonexclusive Remedy for Security Breach. Any failure of the Contract Activities to meet the requirements of this Schedule with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of the Contract for which the State, at its option, may terminate the Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

SCHEDULE Q – MOBILE VIDEO ADDENDUM FOR MOBILE VIDEO PRODUCTS

This Mobile Video Addendum (this “MVA”) is governed by the State of Michigan Contract No. 190000001544 dated October 1, 2019, as amended (“PRIMARY AGREEMENT”), entered into between Motorola Solutions, Inc. and the State of Michigan (“Customer”). Capitalized terms used in this MVA, but not defined herein, will have the meanings set forth in the Primary Agreement.

- 1. Addendum.** This MVA governs Customer’s purchase of any Motorola mobile video Products. A “**Mobile Video System**” is a solution that includes at least one mobile video Product and requires Integration Services to deploy such mobile video Product or the associated evidence management Product at a Customer Site. In addition to the PRIMARY AGREEMENT, the Subscription Services Schedule (“**SSS**”), attached as Schedule H to the PRIMARY AGREEMENT, may be applicable to Products under this MVA with respect to Subscription Software, with respect to Licensed Software and Equipment, as each of those terms are defined therein, and as further described below.
- 2. Evidence Management Systems; Applicable Terms and Conditions.**

 - 2.1. On-Premise Evidence Management.** If Customer purchases a Mobile Video System where Equipment and Licensed Software for evidence management is installed at Customer Sites (an “**On-Premises Evidence Management System**”), then, unless the Ordering Document(s) specify that any software is being purchased on a subscription basis (i.e., as Subscription Software), any (i) Equipment and (ii) Licensed Software installed at Customer Sites or on Customer-Provided Equipment, in each case purchased in connection with the On-Premises Evidence Management System, are subject to the SSS and Primary Agreement. On-Premises Evidence Management Systems described in this Section qualify for the System Warranty as described in **Section 4 – On-Premises Evidence Management System Warranty** (the “**System Warranty**”).
 - 2.2. Cloud Hosted Evidence Management.** If Customer purchases Mobile Video System where the software for evidence management is hosted in a data center and provided to Customer as a service (“**Cloud Hosted Evidence Management System**”), including but not limited to CommandCentral Evidence, VideoManager EX, and VideoManager EL Products, then such Cloud Hosted Evidence Management System is subject to the SSS. Any Equipment purchased in connection with Cloud Hosted Evidence Management System is subject to the Primary Agreement and SSS. Cloud Hosted Evidence Management System described in this Section do not qualify for the System Warranty. System completion, however, is determined in accordance with the provisions of **Section 7 –System Completion** below.
 - 2.3. Services.** Any Integration Services or Maintenance and Support Services purchased in connection with, or included as a part of, a Mobile Video System are subject to the PRIMARY AGREEMENT, and as described in the applicable Ordering Document(s).
- 3. Payment.** Customer will pay invoices for the Products and Services covered by this MVA in accordance with the invoice payment terms set forth in the PRIMARY AGREEMENT. Fees for Mobile Video Systems will be invoiced as of the System Completion Date, unless another payment process or schedule or

milestones are set forth in an Ordering Documents or applicable Addendum. In addition to Equipment, Licensed Software, Subscription Software and Integration Services (as applicable) sold as part of a Mobile Video System, the Ordering Documents for a Mobile Video System may also include post-deployment Integration Services or other Services which are to be provided following the date of functional demonstration (“**Post-Deployment Services**”). Post-Deployment Services will be invoiced upon their completion and paid by Customer in accordance with the terms of the PRIMARY AGREEMENT.

- 4. On-Premises Evidence Management System Warranty.** Subject to the disclaimers in the PRIMARY AGREEMENT and the SSS, Motorola represents and warrants that, on the System Completion Date (as defined below) for an On-Premises Evidence Management System described in **Section 2.1 – On-Premises Evidence Management** (a) such On-Premises Evidence Management System will perform in accordance with the descriptions in the applicable Ordering Documents in all material respects, and (b) if Customer has purchased any Equipment or Motorola Licensed Software (but, for clarity, excluding Subscription Software) as part of such On-Premises Evidence Management System, the warranty period applicable to such Equipment and Motorola Licensed Software will continue for a period of one (1) year commencing upon the System Completion Date for the On-Premises Evidence Management System that includes such Products, or on the applicable Product Completion Date, if earlier. The warranties set forth in the applicable Addenda are not otherwise modified by this MVA.
- 5. Additional Software and Video Terms.**

 - 5.1. Unlimited Storage.** Storage shall be specifically described in an Ordering Documents. In the event Customer purchases a Cloud Hosted Evidence Management System with “Unlimited Storage”, as specified in the Ordering Documents, then “Unlimited Storage” means storage of all data captured using Equipment sold under this MVA., provided that (1) video recordings are recorded in an event-based setting where users are not recording an entire shift under one video footage and (2) Customer’s data retention policies and practices do not result in the retention of data beyond the minimums set forth by the State agency statutorily empowered to determine published retention schedules in which the Customer resides. In the event Customer does not comply with the preceding clauses (1) and (2), Motorola shall have the right to charge Customer for such excess data storage at the prevailing rates. Motorola also has the right to place any data that has not been accessed for a consecutive six (6) month period into archival storage, retrieval of which may take up to twenty-four (24) hours from any access request.
 - 5.2. Applicable End User Terms.** Additional license terms apply to third-party software included in certain software Products, see Exhibit 1 to this Schedule Q – Third Party License Terms and Conditions. If the modified license terms are determined to be materially detrimental to Customer, in the Customer’s sole discretion, then Customer may terminate the Services. For clarity, no State Data will be sent outside of the U.S. through Motorola’s use of third-party software and/or services.
 - 5.3. WatchGuard Detector Mobile.** Any order by Customer of WatchGuard Detector Mobile is on a subscription basis and subject to the SSS.

- 5.4. Vigilant Access.** Customer may opt for subscription to additional Subscription Software, including use of the Law Enforcement Archival Network (“**Vigilant VehicleManager**”), which is subject to the terms and conditions of the SSS and the Vigilant Addendum (attached as Exhibit 2 to this Schedule Q). If Customer purchases a subscription to commercial license plate recognition data, then Customer will comply with the terms of Motorola’s Data License Addendum (attached as Exhibit 3 to this Schedule Q).
- 5.5. License Plate Recognition Data.** License plate recognition (“**LPR**”) data collected by Customer is considered Customer Data (as defined in the PRIMARY AGREEMENT) and is therefore subject to the Customer’s own retention policy. Customer, at its option, may share its LPR data with other similarly situated Law Enforcement Agencies (“**LEAs**”) which contract with Motorola to access Vigilant VehicleManager by selecting this option within Vigilant VehicleManager. Other similarly situated LEAs may similarly opt to share their LPR data with Customer using Vigilant VehicleManager. Such LPR data generated by other LEAs is considered Third-Party Data (as defined in the PRIMARY AGREEMENT), is governed by the retention policy of the respective LEA, and shall be used by Customer only in connection with its use of Vigilant VehicleManager. LPR data that has reached its expiration date will be deleted from Vigilant VehicleManager. Only individuals who are agents and/or sworn officers of Customer and who are authorized by Customer to access Vigilant VehicleManager on behalf of Customer through login credentials provided by Customer (“**User Eligibility Requirements**”) may access Vigilant VehicleManager. Vigilant in its sole discretion may deny access to Vigilant VehicleManager to any individual based on such person’s failure to meet the User Eligibility Requirements. Customer will ensure no user logins are provided to agents or officers of other local, state, or Federal LEAs without the express written consent of Vigilant. Customer will be responsible for its authorized users’ access to, and use of, Vigilant VehicleManager through use of Customer login credentials, including ensuring their compliance with this Agreement. Notwithstanding the foregoing, Motorola is not responsible for the Customer’s authorized users sharing of Customer login credentials.
- 5.6. API Support.** Motorola will use commercially reasonable efforts to maintain its Application Programming Interface (“**API**”) sold in connection with any Mobile Video System. APIs will evolve and mature over time, requiring changes and updates. Motorola will use reasonable efforts to continue supporting any version of an API for six (6) months after such version is introduced, but if Motorola determines, in its sole discretion, to discontinue support of an API for any reason, Motorola will provide reasonable advance notification to Customer. If an API presents a security risk, Motorola may discontinue an API without prior notice.
- 5.7. Support of Downloaded Clients.** If Customer purchases any software Product that requires a client installed locally on Customer-Provided Equipment or Equipment in possession of Customer, Customer will be responsible for downloading and installing the current version of such client, as it may be updated from time to time. Motorola will use reasonable efforts to continue supporting any version of a client for forty-five (45) days following its release, but Motorola may update the current version of its client at any time, including for bug fixes, product improvements, and feature updates, and Motorola makes no representations or warranties that any software Product will support prior versions of a client.

5.8. CJIS Security Policy. Motorola agrees to support Customer's obligation to comply with the Federal Bureau of Investigation Criminal Justice Information Services ("**CJIS**") Security Policy, incorporated herein, and will comply with the terms of the CJIS Security Addendum for the term of the Addendum or Ordering Documents for the applicable Product. Motorola personnel that require access to unencrypted Criminal Justice Information ("CJI") for purposes of Product support and development must be escorted by a MSP authorized user who is authorized unescorted CJI access. In an emergency situation, MSP may provide escorted access via a mutually agreeable virtual method only if strictly necessary and provided such access remains in compliance with CJIS requirements.

6. Reserved.

7. System Completion. Any Mobile Video System sold hereunder will be deemed completed upon Customer's (or the applicable Authorized User's) Beneficial Use of the applicable Mobile Video System (the "**System Completion Date**"). Customer will not unreasonably delay Beneficial Use, and in any event, the Parties agree that Beneficial Use will be deemed to have occurred thirty (30) days after functional demonstration. As used in this Section, "**Beneficial Use**" means use by Customer or at least one (1) Authorized User of the material features and functionalities of Mobile Video System, in material conformance with Product descriptions in the applicable Ordering Documents. Any additional Equipment sold in connection with the initial Mobile Video System shall be deemed delivered in accordance of the terms of the Primary Agreement. Any additional Subscription Software purchased under the VaaS Program will be deemed delivered upon Customer's receipt of credentials required for access to the Cloud Hosted Evidence Management System or upon Motorola otherwise providing access to the Cloud Hosted Evidence Management System. This Section applies to Products purchased under the MVA notwithstanding the delivery provisions of the Addendum applicable to such Products, such as the SSS or Primary Agreement, and this Section will control over such other delivery provisions to the extent of a conflict.

8. Additional Cloud Terms. The terms set forth in this **Section 8 – Additional Cloud Terms** apply in the event Customer purchases any cloud hosted software Products under this MVA, including a Cloud Hosted Evidence Management System.

8.1. Data Storage. Motorola will determine, in its sole discretion, the location of the stored content for cloud hosted software Products. All data, replications, and backups will be stored at a location in the United States for Customers in the United States.

8.2. Data Retrieval. Cloud hosted software Products will leverage different types of storage to optimize software, as determined in Motorola's sole discretion. For multimedia data, such as videos, pictures, audio files, Motorola will, in its sole discretion, determine the type of storage medium used to store the content. The type of storage and medium selected by Motorola will determine the data retrieval speed. Access to content in archival storage may take up to twenty-four (24) hours to be viewable.

8.3. Availability. Unless otherwise specified in the Ordering Documents, Motorola will make reasonable efforts to provide monthly availability of 99.5% for cloud hosted software Products with the exception of maintenance windows.

8.4. Maintenance. Scheduled maintenance of cloud hosted software Products will be performed periodically. Motorola will make commercially reasonable efforts to notify customers one (1) week in advance of any such maintenance. Unscheduled and emergency maintenance may be required from time to time. Motorola will make commercially reasonable efforts to notify customers of any unscheduled or emergency maintenance twenty-four (24) hours in advance.

9. Survival. The following provisions will survive the expiration or termination of this MVA for any reason:
**Section 1 – Addendum; 2 – Evidence Management Systems; Applicable Terms and Conditions;
Section 3 – Payment; Section 5.2 – Applicable End User Terms; Section 9 – Survival.**

SCHEDULE Q - EXHIBIT 1 – THIRD-PARTY LICENSE TERMS AND CONDITIONS

MICROSOFT ON-PREMISE TERMS

1. SOFTWARE LICENSE. As to any Microsoft Products being furnished, the Microsoft software for those Microsoft Products is sublicensed to Licensee from Motorola pursuant to the Customer's Motorola Software License Agreement and is subject to the additional Microsoft End-User License Agreement terms.

2. CUSTOMER USERS. Notwithstanding any provisions herein to the contrary, the following provisions apply concerning the Microsoft Products. If Customer is acquiring from Motorola a Microsoft SQL Server and/or a Microsoft System Center Operations Manager, then Customer warrants 1) that the number of users that may access the System are correctly indicated in the Exhibits to this Agreement; 2) that Customer is not being licensed the SQL Server or Microsoft System Center Operations Manager under a license from Microsoft, but rather under a sublicense from Motorola; 3) that the copies of the referenced Microsoft Products it receives from Motorola do not entitle it to maintain on its computer systems any more copies of the Microsoft Products than it previously licensed from Motorola or Microsoft; 4) that Customer possesses and will maintain sufficient quantities of fully valid Microsoft licenses to support the maximum number of users and/or devices that may access or use the System under the provisions of the End-User License Agreement, 5) that Microsoft will be an intended third party beneficiary of the End-User License Agreement, with the right to enforce the warranties and any other provisions of the End-User License Agreement provisions and to verify compliance of the End User with the same, 6) that Customer shall not run on a mirrored database server for more than 30 days without obtaining a SQL license for that server, 7) that the Customer grants permission for the disclosure of End-User information by Motorola as required in Motorola's Monthly royalty reports and ordering information reports to Microsoft, 8) that Microsoft does not transfer any ownership rights in any Product, and 9) that Motorola is solely responsible for providing technical support for the Microsoft Products.

3. LIMITATIONS. The rights granted in this Agreement with respect to Microsoft Products are subject to the following limitations: 1) Customer has no copyright interest in the Microsoft Products; 2) Customer may not rent, lease, lend or provide hosting services with the Products; 3) Customer may not reverse engineer, decompile or disassemble any Product; 4) Customer may not remove, modify or obscure any copyrights, trademarks or other proprietary right notices contained in the Products; and 5) The Microsoft Products are not designed or intended for use in any situation where failure or fault of the product could lead to death or serious bodily injury of any person, or to severe physical or environmental damage ("High Risk Use"). Motorola's right to sublicense Microsoft Products excludes the right to use, or distribute the Microsoft Products for Customer's use in, or in conjunction with, High Risk Use, therefore, High Risk Use is strictly prohibited. High Risk use, by way of example, includes aircraft or other modes of human mass transportation, nuclear or chemical facilities, and Class III medical devices under the Federal Food, Drug and Cosmetic Act. Notwithstanding the foregoing, as long as PremierOne CAD is used in a manner for which it was designed and in accordance with the documentation provided, Motorola declares such use is not considered to be High Risk Use as defined by Microsoft.

4. MICROSOFT PRODUCTS WARRANTY. Notwithstanding any provisions herein to the contrary, the following provisions apply to the Microsoft Products:

4.1. Microsoft Products are not fault tolerant or free from errors, conflicts, interruptions or other imperfections. Performance may vary depending upon what hardware platform they are installed on, the interactions with other software applications and each product's configurations.

4.2. Microsoft Corporation is providing the Microsoft Products "as-is" with no warranty of any kind and disclaims all warranties, express and implied, to the maximum extent allowed by applicable law. Microsoft further disclaims any liability of Microsoft for any damages, whether direct, indirect incidental or consequential, as a result of the use or installation of the Products. Additionally, to the extent permitted under applicable law, Microsoft Corporation excludes for itself and its suppliers all warranties of any kind, including:

- a. any warranties of title, non-infringement, merchantability and fitness for a particular purpose;
- b. any implied warranty arising from course of dealing or usage of trade;
- c. any common law duties relating to accuracy or lack of negligence with respect to the Microsoft Products, any Master Copy, and any Software Documentation; and
- d. that the products will operate properly in connection with the System, the Motorola products or on any Customer system(s).

If applicable law gives Customer any implied warranties, guarantees or conditions despite the foregoing exclusion, those warranties will be limited to one year and Customer remedies will be limited to the maximum extent allowed by this Agreement.

5. THIRD PARTY PROVIDED DOCUMENTATION. Non-Motorola authored documentation will be provided in the format available from the vendor and in accordance with the vendors distribution policy.

The following third-party terms are applicable to both on-premise & cloud:

TWILIO SERVICES

Twilio may suspend its Services immediately for cause if Twilio, in good faith, determines: (a) that Customer or an Authorized User materially breaches (or Twilio, in good faith, believes that Customer or an Authorized User has materially breached) any provisions of the Agreement relating to Twilio's services ('Services') between Customer and Motorola Solutions, Inc. or its affiliated companies (collectively, "Motorola") (the "Agreement"), or that Customer has breached the [Twilio Acceptable Use Policy](#); (b) there is an unusual and material spike or increase in Customer's use of the Services and that such traffic or use is fraudulent or materially and negatively impacting the operating capability of the Services; (c) that its provision of the Services is prohibited by applicable law or regulation; (d) there is any use of the Services by Customer or an Authorized User that threatens the security, integrity, or availability of the Services; or (e) that Customer or an Authorized User has not provided adequate notices or obtained the necessary permissions and consents to provide Customer Data to Twilio for use and disclosure pursuant to the Twilio [Privacy Policy](#).

Twilio as a Controller of Customer Usage Data. Customer acknowledges that, with regard to the processing of Customer Usage Data, Twilio is an independent controller, not a joint controller with Motorola. Customer grants Twilio and its affiliates the right to process Customer Usage Data solely as necessary to provide the Services in accordance with the Twilio Privacy Policy. Customer is responsible for the quality and integrity of Customer Usage Data. "Customer Usage Data" means data processed by Twilio for the purposes of transmitting or exchanging Customer content, including data used to identify the source and destination of a communication, such as (a) individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the Services, and the date, time, duration and the type of communication and (b) activity logs used to identify the source of Service requests, optimize and maintain performance of the Services, and investigate and prevent system abuse.

DISCLAIMER. TWILIO SERVICES ARE PROVIDED "AS IS," AND NEITHER MOTOROLA NOR TWILIO MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT TO THE FULLEST EXTENT PERMITTED BY LAW. TWILIO AND MOTOROLA ADDITIONALLY DISCLAIM ALL WARRANTIES RELATED TO THIRD PARTY TELECOMMUNICATIONS PROVIDERS. CUSTOMER ACKNOWLEDGES THE INTERNET AND TELECOMMUNICATIONS PROVIDERS' NETWORKS ARE INHERENTLY INSECURE AND THAT TWILIO AND MOTOROLA WILL HAVE NO LIABILITY FOR ANY CHANGES TO, INTERCEPTION OF, OR LOSS OF CUSTOMER DATA WHILE IN TRANSIT VIA THE INTERNET OR A TELECOMMUNICATIONS PROVIDER'S NETWORK.

SCHEDULE Q – EXHIBIT 2 – VIGILANT ADDENDUM

Vigilant Addendum

For Vigilant automated license plate recognition software and hardware Products

This Vigilant Addendum (“**Vigilant Addendum**”) is governed by the State of Michigan Contract No. 190000001544 dated October 1, 2019, as amended (“primary agreement”), entered into between Motorola Solutions, Inc. and the State of Michigan (“Customer”). Capitalized terms used in this Vigilant Addendum, but not defined herein, will have the meanings set forth in the primary agreement or applicable Addendum.

1. Addendum. This Vigilant Addendum governs Customer’s purchase and use of Motorola’s Vigilant automated license plate recognition software and hardware Products (“**LPR Products**”). In addition to the primary agreement, the Subscription Services Schedule (“SSS”) attached as Schedule H to the primary agreement, with respect to Subscription Software for Equipment sold as part of any LPR Products, together with any other applicable terms herein may be applicable to LPR Products offered under this Vigilant Addendum. LPR Products may also include Subscription Software on such Equipment or otherwise made available to Customer, as further described below.

2. Definitions.

Camera License Key (“CLK”) means an electronic key that will permit each camera (one CLK per camera) to be used with Vigilant CarDetector and/or Subscription Software.

Commercial Booking Images refers to booking images collected by commercial sources and available on Vigilant VehicleManager with a paid subscription.

Commercial Data means both Commercial Booking Images and Commercial LPR Data.

Commercial LPR Data refers to LPR data collected by private sources and available on Vigilant VehicleManager with a paid subscription.

License Plate Recognition (“LPR”) refers to the process of utilizing cameras, either stationary or mounted on moving vehicles, to capture and interpret images of vehicle license plates.

3. Subscription Software

3.1. CarDetector. Customer may purchase Vigilant CarDetector which is Subscription Software subject to the SSS. For Customers subscribing to CarDetector, Customer is required to obtain a CLK for each Motorola-approved camera which uses CarDetector. A CLK can be obtained by Customer by going to Motorola’s company support website and completing the online request form to Motorola technical support staff.

3.2. Vigilant VehicleManager and Vigilant ClientPortal. Subject to the terms below, Customer may purchase a CLK for access to the Law Enforcement Archival Report Network (“**VehicleManager**”) and/or the Vigilant ClientPortal (“**ClientPortal**”) each of which are “Subscription Software” subject to the terms of the SSS.

- 3.2.1. Access. Use and access to VehicleManager is strictly restricted to Law Enforcement Agencies (“**LEAs**”) and their Authorized Users. Non-LEAs and their Authorized Users may purchase/access Client Portal.
- 3.2.2. Data Ownership and Retention. Motorola retains all title and rights to Commercial LPR Data and Commercial Booking Images. Customer shall not utilize Commercial LPR Data or Commercial Booking Images on the behalf of other local, state or Federal LEAs. LPR data and where applicable, booking images, collected by the Customer is considered Customer Data (as defined in the primary agreement) and is subject to the Customer’s own retention policy. LPR data and/or booking images that has reached the end of the retention period set by the Customer in ClientPortal or VehicleManager, will be deleted from ClientPortal or VehicleManager in accordance with Customer’s retention policy. Customer retains all rights to LPR data and booking images collected by Customer.
- 3.2.3. Data Sharing. Customer has the option share its Customer Data with LEA’s who contract with Motorola for VehicleManager access. ClientPortal customers may also share its Customer Data with other non-LEA customers who have a contract with Motorola for ClientPortal access. If Customer opts, in its sole discretion, to share such data with another customer, the sharing Customer thereby grants to the recipient customer the rights to use such data in accordance with the terms of VehicleManager or Client Portal, as applicable.
- 3.2.3.1. LEA Customers. If Customer is an LEA, other similarly situated LEAs that collect their own LPR data and booking images may opt to share such data with Customer using VehicleManager. Additionally, Non-LEA Client Portal customers may also share their own LPR data with LEA Customer. Such LPR data or booking images generated by other LEAs or Non-LEA customers is considered Third-Party Data (as defined in the primary agreement) and shall be used by Customer only in connection with its use of VehicleManager. Third-party LPR data or booking data is governed by the retention policy of its respective owner, once the Third Party LPR or booking data has reached its expiration date will be deleted from VehicleManager/Client Portal in accordance with the retention terms of the sharing agency.
- 3.2.3.2. Non-LEA Customers. If Customer is a non-LEA Customer, other similarly situated ClientPortal customers that collect their own LPR data may opt to share such data with Customer using ClientPortal. Such LPR data generated by other ClientPortal customers is considered Third-Party Data (as defined in the primary agreement), is governed by the retention policy of the respective ClientPortal customer, and shall be used by Customer only in connection with its use of ClientPortal. Third-party LPR data that has reached its expiration date will be deleted from ClientPortal in accordance with the retention terms of the sharing entity.
- 3.2.4. Motorola in its sole discretion may deny access to ClientPortal or VehicleManager to any individual based on such person’s failure to satisfy the requirements set forth

hereunder. Customer will ensure no user logins are provided to agents or officers of other local, state, or Federal LEAs without the express written consent of Motorola. Customer will be responsible for all of its Authorized Users, and use of, ClientPortal or VehicleManager through use of Customer login credentials, including ensuring their compliance with this Addendum. Customer shall notify Motorola promptly if Customer believes the password of any of its Users has, or may have, been obtained or used by any unauthorized person(s). In addition, Customer must notify Motorola promptly if Customer becomes aware of any other breach or attempted breach of the security of any of its Users' accounts.

3.2.5. Commercial Data Access. If Customer purchases a subscription to Commercial Data, then Customer shall comply with the terms of Motorola's Data License Addendum (attached as Exhibit 3 to Schedule Q).

3.2.6. CJIS Security Policy. Motorola agrees to support a law enforcement Customer's obligation to comply with the Federal Bureau of Investigation Criminal Justice Information Services ("CJIS") Security Policy and will comply with the terms of the CJIS Security Addendum for the term of the Addendum or Ordering Document for the applicable Product. Motorola personnel that require access to unencrypted Criminal Justice Information ("CJI") for purposes of Product support and development must be escorted by a MSP authorized user who is authorized unescorted CJI access. In an emergency situation, MSP may provide escorted access via a mutually agreeable virtual method only if strictly necessary and provided such access remains in compliance with CJIS requirements.

4. Survival. The following provisions will survive the expiration or termination of this Vigilant Addendum for any reason: Section 1 – Addendum; Section 3 – Subscription Software; Section 4 – Survival.

SCHEDULE Q – EXHIBIT 3 – DATA LICENSE ADDENDUM

Data License Addendum¹

This Data License Addendum (this “**DLA**”) is governed by the State of Michigan Contract No. 190000001544 dated October 1, 2019, as amended (“**Primary Agreement**”), entered into between Motorola Solutions, Inc. and the State of Michigan (“**Customer**”). Capitalized terms used in this DLA, but not defined herein, will have the meanings set forth in the **Primary Agreement**.

- 1. Addendum.** This DLA governs Customer’s license of Licensed Data from Motorola, and shall form part of the Parties’ **Primary Agreement**. “**Licensed Data**” means Motorola Data, Third-Party Data, or a combination of Motorola Data and Third-Party Data ordered by Customer under this DLA, as set forth in an Ordering Document.
- 2. Delivery of Licensed Data.**
 - 2.1. Delivery.** Following commencement of the applicable Data License Term (as defined in an Ordering Document), Motorola will provide to Customer the Licensed Data via an electronic means of delivery offered by Motorola (such as a data file or access via a subscription-based Product or online portal) (“**Delivery Method**”).
 - 2.2. Modifications.** In addition to other rights to modify the Products and Services set forth elsewhere in the Agreement, Motorola (or its third-party data providers) may modify the Licensed Data, at its sole discretion. Motorola may modify Delivery Methods at any time. In the event of a material change in delivery method, parties may be subject to a mutually negotiated Contract Change Notice. Enhancements or additions to Licensed Data or Delivery Methods may be subject to additional Fees, which shall be mutually agreed upon in a Change Order by the Parties. If the modifications to the Licensed Data and Delivery Methods are determined to be materially detrimental to Customer, in the Customer’s sole discretion, then Customer may terminate the Services in accordance with the primary agreement.
- 3. Licensed Data Use and Restrictions.** As between Motorola and Customer, Motorola is the owner of all Licensed Data. Subject to Customer’s and its End Users’ (as defined in the Ordering Document, if applicable) compliance with the Agreement (including payment terms), Customer is permitted to (a) access the applicable Delivery Method for purposes of accessing the Licensed Data in accordance with this DLA and the Ordering Document, and (b) Customer may use Licensed Data solely in accordance with the License Scope specified in the applicable Ordering Document. Unless expressly permitted in the applicable Ordering Document, use of Licensed Data is subject to the restrictions set forth in the **Primary Agreement**, and any other restrictions set forth in the Agreement or as required by a third-party data provider. If a third-party data provider and Customer enter into a separate agreement governing use

¹ For any DRN data licenses, the DRN version of this document applies

of certain Third-Party Data, then such separate agreement will control over this DLA in the event of a conflict, solely with respect to such Third-Party Data.

- 4. Display of Licensed Data.** Customer will not display Licensed Data unless agreed to by the Parties in a Contract Change Notice incorporating the applicable terms for displaying Licensed Data.
- 5. Term.**
 - 5.1. Term.** The term of this DLA (the “**DLA Term**”) will commence upon the date set forth on the Contract Change Notice to the Primary Agreement when ordering any Licensed Data. In addition to Motorola’s other termination rights under the Primary Agreement, Motorola has the right to terminate the license to any Licensed Data in the event Licensed Data includes Third Party Data and Motorola’s license to such data is terminated or modified by the applicable third-party data provider, or if a third-party data provider fails to provide Third Party Data to Motorola, and Motorola may reduce the scope of the applicable Ordering Document accordingly.
 - 5.2. Effect of Termination.** Upon termination or expiration of this DLA, or an Ordering Document, Customer’s rights to the applicable Licensed Data (including any rights to use Motorola or third-party data provider marks or other brand features in accordance with **Section 4.3**) will terminate, and in accordance with the Primary Agreement, Customer and all End Users will immediately discontinue use of such Licensed Data and marks and other brand features, delete all copies thereof, and certify such deletion to Motorola.
- 6. Payment.** Customer will pay the License Fee set forth in each Ordering Document for the applicable Licensed Data described therein. Payment is in accordance with the Primary Agreement.
- 7. License True-Up.** Motorola will have the right to conduct an audit of Customer’s use of the Licensed Data during the applicable Data License Term (as set forth in the applicable Ordering Document), and Customer will cooperate with such audit. If Motorola determines that Customer’s usage of the Licensed Data during the applicable Data License Term does not comply with the terms of the Agreement, including this DLA, Motorola may invoice Customer for the additional or nonconforming usage by Customer, and Customer will pay such invoice in accordance with the payment terms in the Primary Agreement.
- 8. Security and Confidentiality.** Unless expressly permitted in an Addendum or Ordering Document, Customer will not disclose Licensed Data to third parties, and in all cases, Customer will use best efforts, including by implementing industry standard security measures, to protect and secure Licensed Data and guard against unauthorized disclosure and use.
- 9. Reserved.**
- 10. Disclaimer.** IN ADDITION TO THE DISCLAIMERS SET FORTH IN THE PRIMARY AGREEMENT, AND NOTWITHSTANDING ANY PROVISION OF THE AGREEMENT TO THE CONTRARY, MOTOROLA IS NOT RESPONSIBLE FOR (AND WARRANTIES AND INDEMNITIES DO NOT APPLY TO) THE LICENSED DATA, AND CUSTOMER AGREES THAT THE LICENSED DATA IS PROVIDED AS-IS AND WITHOUT WARRANTY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE, AND CUSTOMER MUST EXERCISE INDEPENDENT JUDGMENT WHEN USING THE LICENSED DATA TO ENSURE THAT THEY ARE SUITABLE FOR THE CUSTOMER

APPLICATION OR CUSTOMER'S OTHER NEEDS AND THAT THE LICENSED DATA IS SUITABLE AND SAFE FOR END USERS AND OTHER THIRD PARTIES. WITHOUT LIMITING THE FOREGOING, LICENSOR DOES NOT WARRANT THAT ALL ERRORS CAN BE CORRECTED, OR THAT AVAILABILITY OF THE LICENSOR CONTENT SHALL BE UNINTERRUPTED, ACCURATE, COMPLETE, OR ERROR-FREE.

- 11. Survival.** The following provisions will survive the expiration or termination of this DLA for any reason: **Section 5** (Term); **Section 6** (Payment); **Section 7** (Audit; Review); **Section 8** (Security Confidentiality); **Section 10** (Disclaimer); **Section 11** (Survival).

ATTACHMENT 1 – SCHEDULE L- STATEMENT OF WORK ADDITIONS

Contract No. 190000001544
Michigan State Police (MSP)
Vesta 9-1-1 System

Attachment 1 – Schedule L – Statement of Work Additions (Effective 12/17/2024 via Change Notice No. 10).

Assumptions:

- A full Authority to Operate (ATO) must be completed by January 3, 2025. Contractor must participate in the ATO process and provide singular line-item responses regarding the ATO process on or before January 3, 2025. Should the Contractor need to work with a third party to gain responses or information necessary for the /ATO process, the due date of January 3, 2025, shall still apply. Any ATO questions by Contractor or third-party representatives requesting clarification will receive a response from MSP within three (3) business days.
- The State of Michigan will not support use of or monitoring by the Motorola Public Safety Threat Alliance (PSTA). Once the ATO has been approved by the State and VESTA is allowed to proceed with it's go live functions, the PSTA service from Motorola will not be utilized.

Payment Schedule:

- Vendor requests \$53,500 to have their internal staff answer required questions provided by the SOM to finalize the ATO approval. This approval is required prior to any product going live by any SOM Departments.
- Vendor has a \$35,973.56 credit with The SOM currently on CN #7 MA#1900000001544. Vendor is requesting an additional \$17,526.44 to supplement their time answering the ATO questions.
- This additional amount is only for Motorola staff to answer the needed questions produced by the SOM for ATO purposes. It is not to be used for anything else.

ATO Professional Services Hours	\$53,500.00
MSP VESTA Credit Remaining from CN#7	\$35,973.56
Remaining Balance Due and Requested Contract Value Increase	\$17,526.44

Expenses:

- There will be no continuous costs associated with this one-time effort. Funding is only for the one-time use of obtaining ATO approval.

- If more money is needed beyond original agreed upon \$53,000 to finalize the ATO process with the SOM, then Motorola shall work with SOM to figure out how much will be needed to finish Motorola work to obtain ATO approval.
- If there is a money left over from the original agreed upon \$53,000 amount than Motorola shall reduce the FY2026 VESTA annual warranty and maintenance fees by the credit left from this unused amount.



**STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES**

Department of Technology, Management, and Budget
320 S. WALNUT ST., LANSING, MICHIGAN 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **9**
to
Contract Number **190000001544**

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago, IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Kate Jannereth	DTMB
		517-881-1031	
		jannerethk@Michigan.gov	
	Contract Administrator	Alannah Doak	DTMB
		(517) 230-9424	
		doaka@michigan.gov	

CONTRACT SUMMARY

MPSCS CONTINUED SYSTEM UPDATES, EQUIPMENT, MAINTENANCE AND UPGRADES, AND ANCILLARY SYSTEMS PRODUCTS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
October 1, 2019	December 31, 2029	0 - 0 Year	December 31, 2029
PAYMENT TERMS		DELIVERY TIMEFRAME	
NET 45		As per Delivery Order	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

As per Delivery Order

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		December 31, 2029
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$102,215,096.00	\$0.00	\$102,215,096.00		

DESCRIPTION

Effective 2/14/2024, this contract is adding scope to Schedule A via Attachment 11 - Public Safety Threat Alliance Subscription Services.

All other terms, conditions, specifications and pricing remain the same. Per Contractor and Agency agreement and DTMB Central Procurement Services approval.

**Program Managers
for
Multi-Agency and Statewide Contracts**

AGENCY	NAME	PHONE	EMAIL
DTMB	Kate Jannereth	517-881-1031	JannerethK@michigan.gov
MSP	Jonathon Whitford	517-512-4068	WhitfordJ@michigan.gov

CHANGE NOTICE #9

SCHEDULE A, ATTACHMENT 11

STATEMENT OF WORK FOR PUBLIC SAFETY THREAT ALLIANCE SUBSCRIPTION SERVICES

These Subscription Services for Public Safety Threat Alliance (“Agreement”) will be governed by the State of Michigan Contract No. 190000001544 dated October 1, 2019, as amended (“Primary Agreement”), including the terms and conditions in Schedule H – Subscription Services Schedule, entered into between Motorola Solutions, Inc. and the State of Michigan (“Customer”). Capitalized terms used below, but not defined herein, will have the meaning set forth in the Primary Agreement and related Schedule H – Subscription Services Schedule.

1. Definitions

“**Content Materials**” are anonymized, aggregated and/or other generalized information obtained from Public Safety Threat Alliance customers, Motorola customers and other external sources relating to security threat intelligence and mitigation data generally. Such Content Material may include, but is not limited to: 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, as well as tactics, techniques, and procedures used, learned or developed in the course of addressing security incidents.

“**Other Sources**” means (i) other Public Safety Threat Alliance Members or Customers; and (ii) entities and agencies other than Public Safety Threat Alliance Members or Customers, with which Content Material is shared and exchanged for purposes of cybersecurity awareness and preparedness. Other Sources may include Information Sharing and Analysis Centers (ISAC), Information Sharing and Analysis Organizations (ISAO), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), as well as other recognized cybersecurity and infrastructure security organizations. Other Sources may also include specific Motorola teams, including the ActiveEye™ Managed Detection and Response product team, as well as engineering and enterprise information security personnel who have a need to know to provide support for the Public Safety Threat Alliance and for the development and improvement of Motorola’s cybersecurity products and services. Content Material shared with Other Sources is provided subject to appropriate confidentiality and nondisclosure restrictions.

“**Sub-processor**” means other processors engaged by Motorola to Process Content Material.

2. Public Safety Threat Alliance Participation

2.1 Customer Participation. As a Customer participating in the Public Safety Threat Alliance, and as governed by the terms herein, Customer agrees to: (1) provide Content Material to Motorola only as necessary for use by the Public Safety Threat Alliance for purposes consistent with Public Safety Threat Alliance activities and goals, and in Customer’s sole discretion; (2) the aggregation of such Content Material with Content Material derived from Other Sources, and/or (3) the Processing, use and distribution of such Content Material to Other Sources; and/or (4) Motorola’s internal use of Content Materials for its lawful business purposes, including supporting Public Safety Threat Alliance Customers, and improving Motorola products and services. Motorola will not

sell Content Material, make it available in any form or format to unaffiliated third parties that are not Other Sources, or use Content Material for advertising, sales, or marketing purposes. In exchange for Customer's participation hereunder, Motorola will provide Customer access to and use of Content Material from Other Sources, subject to the terms and conditions set forth in this Agreement.

3. Customer Obligations

3.1. Content and Data Sharing. Customer agrees to (1) actively share, in its sole discretion, with Motorola its own properly anonymized, aggregated or generalized information as relevant to the Content Material, and for proposed inclusion and distribution as Content Material for the Public Safety Threat Alliance and (2) to allow for processing of underlying security threat intelligence information as may be identified in any active monitoring or cyber related engagement between Motorola and Customer.

3.2 License and Use of Public Safety Threat Alliance Content Material. Motorola grants Customer a limited, non-transferable, non-sublicensable, and non-exclusive license to use the Content Material solely for the Customer's internal business purposes and only for security related functions. Except as it relates to the Customer's own information and subject to those rights granted under other agreements with Motorola, the Content Material, including any information contributed by other Customers, Motorola customers or third parties, is or becomes the property of Motorola for the benefit of the Public Safety Threat Alliance and may be included in the Content Material. The Content Material is provided for the purpose of use by the Public Safety Threat Alliance and its customers. Customer will not, and require it's Authorized Users to not: (a) use the Content Material, or derivative information therefrom, for any purpose other than Customer's internal business purposes; (b) disclose the Content Material, or derivative information therefrom, to third parties; (c) "white label" the Content Material, or derivative information therefrom or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (d) use such Content Material, or derivative information therefrom, 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 Content Material; or (f) modify such Content Material, or derivative information therefrom, or combine any of it with Customer's own data or other data or use the data to build databases. Customer acknowledges having been advised that the Content Material, or derivative information therefrom, is protected in the U.S. and internationally by a variety of laws, including but not limited to, copyright laws and treaty provisions, trademark laws, patent laws and other proprietary rights laws.

3.3 Confidentiality of the Content Material. The Content Material and other information shared by Customer and Motorola for the benefit of the Public Safety Threat Alliance is deemed to be confidential and "sensitive", in accordance with Addendum A. Customer will: (i) maintain the confidentiality of the Content Material and not disclose it to any third party, except as authorized by the Motorola in writing or as required by a court of competent jurisdiction; (ii) restrict disclosure of the Content Material to its employees who have a "need to know" and not copy or reproduce the Content Material; (iii) take necessary and appropriate precautions to guard the confidentiality of the Content Material, including informing its employees who handle the Content Material that it is confidential and is not to be disclosed to others, but those precautions will be at least the same degree of care that the Customer applies to its own confidential information and will not be less than reasonable care.

4. Public Safety Threat Alliance - Motorola Obligations

4.1 Public Safety Threat Alliance Content Material. Motorola will aggregate Customer provided Content Material with other Content Material collected from Other Sources. Motorola will share the Content Material with Customer and Other Sources, subject to the terms of this

Agreement.

4.2 Anonymization of Content Material. When Content Material is provided by Customer to Motorola for inclusion and distribution through the Public Safety Threat Alliance, Motorola shall have the right to use and distribute such Content Material without further anonymization. Notwithstanding the foregoing, Motorola reserves the right to further anonymize, generalize or aggregate any such provided information, in its sole discretion, prior to release and distribution as part of the Content Material. For avoidance of doubt, Motorola has the sole and absolute discretion relating to the inclusion or exclusion of information from the Content Material and may edit, modify, revise, shorten or choose not to use proposed contributions of information offered from Customer or Other Sources.

4.3 Grant of License to Content Material by Customer. Customer grants Motorola, its subcontractors and Sub-Processors a royalty-free, worldwide, non-exclusive license to use, Process, host, cache, store, reproduce, copy, modify, combine, analyze, create derivative works from Content Material from Customer and to sub-license, communicate, transmit, and distribute such Content Material to other Public Safety Threat Alliance customers in connection with furtherance of the purposes set forth in the Recitals to this Agreement.

5. Motorola Processing of Content Materials

5.1 Motorola's Processing of Content Materials. Motorola and Customer agree that Motorola may only use and Process Content Material, in accordance with applicable law and Customer's documented instructions for the following purposes: (i) to perform under the Agreement including but not limited to as set forth in section 4 above; and (ii) analyze Data to operate, maintain, manage, and improve the Public Safety Alliance. Motorola and Customer agree that this Agreement and Customer's use of the Content Material are Customer's complete and final documented instructions to Motorola for the Processing of Content Materials. Any additional or alternate instructions must be agreed to in writing as an amendment to this Agreement. Content Materials may be processed by Motorola at any of its U.S. locations and/or disclosed to Sub-processors.

5.2 Details of Processing. All Content Materials processed by Motorola through the Public Safety Threat Alliance shall be for purposes described herein and only for the duration of the operation of the Public Safety Threat Alliance.

5.4 Disclosure of Processed Data. Customer agrees Motorola may disclose and share any Content Materials with Other Sources, in Motorola's discretion, to further the purposes of the Public Safety Threat Alliance. In the event a government or supervisory authority demands access to Content Material, to the extent allowable by law, Motorola will 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 with respect to Customer Data, and will contractually obligate its sub-processors to a duty of confidentiality, with respect to the handling of Customer Data contained in Content Materials.

5.7 Sub-processors.

5.7.1 Use of Sub-processors. See Primary Agreement Schedule H, Section 7.3.3.

5.7.2 Changes to Sub-processing. The Customer hereby consents to Motorola engaging the list of Sub-processors as set forth in **Annex II** to process Customer Data provided that: (i) Motorola must provide thirty (30) days written prior notice of the addition or removal of any

Sub-processor; (ii) Motorola imposes data protection terms on any Sub-processor it appoints that protect the Customer Data to the same standard provided for by these terms and the Primary Agreement; 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 the applicable subscription services.

5.8. Motorola Contact. If Customer believes that Motorola is not adhering to its privacy or security obligations hereunder, Customer may contact the Motorola Data Protection Officer at Motorola Solutions, Inc., 500 W. Monroe, Chicago, IL USA 90661-3618 or at privacy1@motorolasolutions.com.

ADDENDUM A - Traffic Light Protocol Labelling

Public Safety Threat Alliance furnished Intelligence information shall not include classified information. The Customer and Motorola agree that all information submitted, processed, stored, archived, or disposed of on or through Public Safety Threat Alliance is "sensitive" information. and to the best of its ability will be labeled and handled in accordance with the [U.S. Department of Homeland \("DHS"\) Security classification guidelines](#) (Traffic Light Protocol (TLP)).

The TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).

TLP labels and their definitions are not intended to have any effect on freedom of information or "sunshine" laws in any jurisdiction.

The source is responsible for ensuring that recipients of TLP information understand and can follow TLP sharing guidance.

If a recipient needs to share the information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source.

Definitions:

TLP: Red - Not for disclosure, restricted to participants only.

TLP: Amber+Strict - Limited disclosure, restricted to participants' organization.

TLP: Amber - Limited disclosure, restricted to participants' organization and its clients

TLP: Green - Limited disclosure, restricted to the community.

TLP: Clear - Disclosure is not limited.

TLP:Red:

When should it be used? Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.

How should it be shared? Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:Amber+Strict

When should it be used? Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.

How should it be shared? Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.

TLP:Amber

When should it be used? Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.

How should it be shared? Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.

TLP:Green

When should it be used? Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.

How should it be shared? Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.

TLP:Clear

When should it be used? Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

How should it be shared? Recipients may share this information without restriction. Information is subject to standard copyright rules.

Other Usage

How to use TLP in email

TLP-designated email correspondence should indicate the TLP color of the information in the Subject line and in the body of the email, prior to the designated information itself. The TLP color must be in capital letters: TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:CLEAR.

How to use TLP in documents

TLP-designated documents should indicate the TLP color of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP color should appear in capital letters and in 12 pt type or greater.

RGB:

TLP:RED : R=255, G=0, B=51, background: R=0, G=0, B=0

TLP:AMBER : R=255, G=192, B=0, background: R=0, G=0, B=0

TLP:GREEN : R=51, G=255, B=0, background: R=0, G=0, B=0

TLP:CLEAR : R=255, G=255, B=255, background: R=0, G=0, B=0

CMYK:

TLP:RED : C=0, M=100, Y=79, K=0, background: C=0, M=0, Y=0, K=100

TLP:AMBER : C=0, M=25, Y=100, K=0, background: C=0, M=0, Y=0, K=100

TLP:GREEN : C=79, M=0, Y=100, K=0, background: C=0, M=0, Y=0, K=100

TLP:CLEAR : C=0, M=0, Y=0, K=0, background: C=0, M=0, Y=0, K=100

ANNEX II

List of Sub-Processors:

Cyware



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 320 S. WALNUT ST., LANSING, MICHIGAN 48933
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **8**
 to
 Contract Number **190000001544**

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago, IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Various	MULTI
STATE	Contract Administrator	Valerie Hiltz	DTMB
		(517) 249-0459	
		hiltzv@michigan.gov	

CONTRACT SUMMARY

MPSCS CONTINUED SYSTEM UPDATES, EQUIPMENT, MAINTENANCE AND UPGRADES, AND ANCILLARY SYSTEMS PRODUCTS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
October 1, 2019	December 31, 2029	0 - 0 Year	December 31, 2029
PAYMENT TERMS		DELIVERY TIMEFRAME	
NET 45		As per Delivery Order	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS
 As per Delivery Order

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		December 31, 2029
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$99,900,000.00	\$0.00	102,215,096.00		

DESCRIPTION
 Effective 9/13/2023 this contract is revising Schedule B.1. for MPSCS as attached.
 All other terms, conditions, specifications and pricing remain the same per Contractor and MPSCS agreement and DTMB Central Procurement Services approval.

**Program Managers
for
Multi-Agency and Statewide Contracts**

AGENCY	NAME	PHONE	EMAIL
DTMB	Kate Jannereth	517-881-1031	JannerethK@michigan.gov
MSP	Jonathon Whitford	517-512-4068	WhitfordJ@michigan.gov

STATE OF MICHIGAN

Michigan's Public Safety Communication System (PMSCS) Continued System Updates, Equipment Maintenance and Updates, and Ancillary Systems Products
SCHEDULE B.1. - PRICING- MPSCS

	COMPONENT	10/1/2019	10/1/2020	10/1/2021	10/1/2022	10/1/2023	10/1/2024	10/1/2025	10/1/2026	10/1/2027	10/1/2028	TOTAL
MPSCS ASTRO LIFECYCLE	System Upgrade Agreeemnt II (SUA II)	\$ 4,666,781.89	\$ 5,119,186.80	\$ 5,570,726.31	\$ 5,900,187.68	\$ 6,460,906.70	\$ 6,502,411.06	\$ 6,545,043.90	\$ 6,589,066.01	\$ 6,634,415.11	\$ 6,681,002.78	\$ 60,669,728.24
	Security Update Services (SUS)	\$ 100,785.87	\$ 103,809.45	\$ 106,923.73	\$ 118,189.84	\$ 121,735.54	\$ 125,387.60	\$ 135,019.65	\$ 139,070.24	\$ 143,242.35	\$ 147,539.62	\$ 1,241,703.89
	Technical Support (TS)	\$ 252,878.41	\$ 260,464.76	\$ 268,278.70	\$ 296,546.12	\$ 305,442.50	\$ 314,605.77	\$ 338,773.22	\$ 348,936.41	\$ 359,404.51	\$ 370,186.64	\$ 3,115,517.04
	OPSOC	\$ 34,839.75	\$ 35,884.94	\$ 36,961.49	\$ 40,855.97	\$ 42,081.65	\$ 43,344.10	\$ 46,673.71	\$ 48,073.92	\$ 49,516.14	\$ 51,001.63	\$ 429,233.30
	Busines Relationship Manger (BRM)	\$ 260,000.00	\$ 267,800.00	\$ 275,834.00	\$ 284,109.02	\$ 292,632.29	\$ 301,411.26	\$ 310,453.60	\$ 319,767.21	\$ 329,360.22	\$ 339,241.03	\$ 2,980,608.63
	TOTAL	\$ 5,315,285.92	\$ 5,787,145.95	\$ 6,258,724.23	\$ 6,639,888.63	\$ 7,222,798.68	\$ 7,287,159.79	\$ 7,375,964.08	\$ 7,444,913.79	\$ 7,515,938.33	\$ 7,588,971.70	\$ 68,436,791.10
TRUE UP	True Up 10-01-21 to 09-30-29 integrations			\$ 78,583.61	\$ 468,078.64	\$ 686,602.80	\$ 705,746.39	\$ 725,535.98	\$ 745,917.17	\$ 766,904.45	\$ 788,517.97	\$ 4,965,887.01
TRUE UP	True Up 10-01-22 to 09-30-29 integrations					\$ 103,591.78	\$ 571,378.84	\$ 589,948.65	\$ 607,647.11	\$ 625,876.52	\$ 644,652.82	\$ 3,143,095.72
TRUE UP	True Up 10-01-22 to 09-30-29 integrations					\$ 162,855.67	\$ 595,288.30	\$ 775,063.98	\$ 806,066.54	\$ 838,309.20	\$ 838,309.20	\$ 3,177,583.69
CRITIAL CONNECT	Critical Connect			\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 760,320.00
	Astro Connectivity Managed Service			\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 458,400.00
	System Upgrade Agreement II (SUA II)				\$ 35,596.00	\$ 36,664.00	\$ 37,764.00	\$ 38,897.00	\$ 40,064.00	\$ 41,266.00	\$ 42,503.00	\$ 272,754.00
	Security Update Services (SUS)				Included	Included	Included	Included	Included	Included	Included	Included
	TOTAL			\$ 152,340.00	\$ 187,936.00	\$ 189,004.00	\$ 190,104.00	\$ 191,237.00	\$ 192,404.00	\$ 193,606.00	\$ 194,843.00	\$ 1,491,474.00
MPSCS PREMIER**	PremierOne CAD		\$ 106,678.14	\$ 109,878.36	\$ 119,812.29	\$ 123,406.92	\$ 127,108.85	\$ 135,644.68	\$ 139,714.22	\$ 143,905.79	\$ 148,222.50	\$ 1,154,371.75
	PremierMDC	\$ 162,778.86	\$ 150,358.48	\$ 154,869.30	\$ 171,187.28	\$ 176,322.96	\$ 181,612.64	\$ 195,563.48	\$ 201,430.32	\$ 207,472.88	\$ 213,696.68	\$ 1,815,292.88
	Upgrade- Hardware / Software / Services		\$ 142,848.92	\$ 142,848.92	\$ 153,301.28	\$ 153,301.28	\$ 153,301.28	\$ 160,269.52	\$ 160,269.52	\$ 160,269.52	\$ 160,269.52	\$ 1,386,679.76
	TOTAL	\$ 162,778.86	\$ 399,885.54	\$ 407,596.58	\$ 444,300.85	\$ 453,031.16	\$ 462,022.77	\$ 491,477.68	\$ 501,414.06	\$ 511,648.19	\$ 522,188.70	\$ 4,356,344.39
OTHER ADD ONS	Lab as a Service (Five Year Agreement)		\$ 655,000.00	\$ 674,650.00	\$ 694,890.00	\$ 715,736.00	\$ 737,208.00					\$ 3,477,484.00
	Lab as a Service (Four Year Agreement)							\$ 761,167.26	\$ 785,905.20	\$ 811,447.11	\$ 837,819.15	\$ 3,196,338.72
	CommandCenter Aware				\$ -	\$ -	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 102,490.00
	Learning Subscription Astro/Cyber					\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 142,653.00
	Astro 25 System Manager				\$ 93,333.33	\$ 258,125.00	\$ 266,514.06	\$ 275,175.77	\$ 284,118.98	\$ 293,352.85	\$ 302,886.82	\$ 1,773,506.81
	TOTAL		\$ 655,000.00	\$ 674,650.00	\$ 788,223.33	\$ 997,636.50	\$ 1,047,995.56	\$ 1,080,616.53	\$ 1,114,297.68	\$ 1,149,073.46	\$ 1,184,979.47	\$ 8,692,472.53
GRAND TOTALS		\$ 5,478,064.78	\$ 6,842,031.49	\$ 7,571,894.42	\$ 8,528,427.45	\$ 9,652,664.92	\$ 10,427,263.02	\$ 11,050,068.22	\$ 11,381,657.79	\$ 11,569,113.49	\$ 11,762,462.86	\$ 94,263,648.44



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 320 S. WALNUT ST., LANSING, MICHIGAN 48933
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number 7
 to
 Contract Number 190000001544

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago, IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Kate Jannereth	DTMB
		517-881-1031	
		jannerethk@Michigan.gov	
	Contract Administrator	Valerie Hiltz	DTMB
		(517) 249-0459	
		hiltzv@michigan.gov	

CONTRACT SUMMARY

MPSCS CONTINUED SYSTEM UPDATES, EQUIPMENT, MAINTENANCE AND UPGRADES, AND ANCILLARY SYSTEMS PRODUCTS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
October 1, 2019	December 31, 2029	0 - 0 Year	December 31, 2029
PAYMENT TERMS		DELIVERY TIMEFRAME	
NET 45		As per Delivery Order	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

As per Delivery Order

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		December 31, 2029
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$99,900,000.00	\$2,315,096.00	\$102,215,096.00		

DESCRIPTION

Effective September 1, 2023 this contract is adding Schedule L- Vesta Phone System for Michigan State Police and the associated funding in the amount of \$2, 315,096.00

All other terms, conditions, specifications and pricing remain the same.

Per Contractor and MSP agreement, DTMB Central Procurement Services agreement, and the approval of the State Administrative Board on August 22, 2023.

Added Via CN # 7, Effective 9/1/23

MA 19000001544

SCHEDULE L

**Michigan State Police (MSP)
 Vesta 9-1-1 System
 Statement of Work (SOW)**

Scope of Work

This Schedule incorporates the planning and implementation of the Contractor’s Next Generation 9-1-1 (NG9-1-1) VESTA 9-1-1 system. The scope of work to be included is:

- Phase 1- Planning
- Phase 2- Installation and Testing
- Phase 3- Cut Over
- Phase 4- Initial Project Wrap-up
- Phase 5- Maintenance

Program Managers

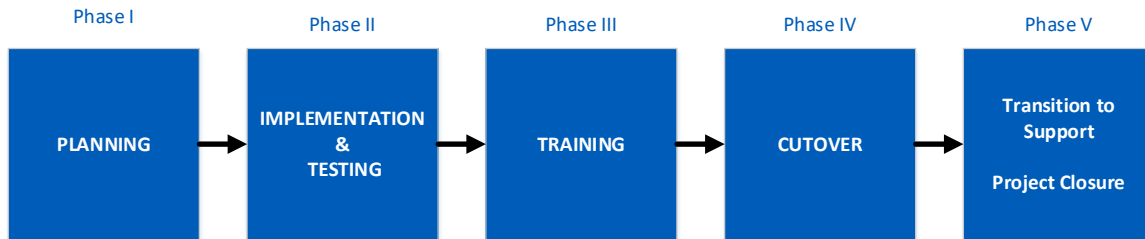
The Project Managers for this work are identified as follows:

For MSP	For the Contractor
Jonathon Whitford Michigan State Police Headquarters witfordj@michigan.gov 517-512-4068	TBD (and provided to the Agency Program Manager) Name Address Email Address Phone #

Implementation Methodology

The State’s MSP Program Manager and the Contractor’s (Project) Manager will play a particularly important role in this process by communicating back to their teams the project plan, project status, risks, and next steps. The project will use an MS Project Schedule and Project Status Report, which will provide a consistent vehicle for communication, management, reporting of progress and detection of potential progress delays.

The Contractors project management methodology is also based upon the Project Management Institute’s (PMI) Project Management Body of Knowledge (PMBOK). Our methodology will incorporate one primary goal; align the project with your overall expectations. Unless otherwise requested, Motorola Solutions will implement the project using a “phased” process.



1.1 Phase I - Planning

Phase I is the period in which the project is formally launched, the project design is finalized, the Project Management Plan (PMP) is finalized, and resources are scheduled.

- A. The Contractors Program Manager will coordinate Phase 1 activities with the MSP Program Manager to ensure that the project scope has been assessed, and that all deliverables have been captured in the Motorola Solutions Project Schedule. The PMP will be the control document for Motorola Solutions deliverables for the implementation, as will other critical dates or milestones that are integral to the project.
- B. The specific objectives of the planning phase include:
 - 1. Expound on specific strategies and project options
 - 2. Confirm NG9-1-1 project scope
 - 3. Finalize the solution design
 - 4. Finalize plans for solution delivery strategies and resources. The solution is reviewed to align each primary stakeholder with a common vision and strategy for unified team design and planning.
 - 5. Determine aspects of the 9-1-1 system that are subject to change within the scope of the project. Much of this entails identifying and collecting information from project stakeholders.
- C. Prior to collecting the detailed information that will be used in the course of the project, it is important for the team to understand the overall project goals and the criteria that will govern their decision-making.
- D. The project principles and constraints are communicated to all team members so that all design, integrations, and deployment decisions can be assessed. Guided by the project principles and constraints, more detail information is then collected. This includes conducting site visits and the Project Launch, Call Flow and Design Review Meeting.
- E. The original configuration proposed was based on information provided by Michigan State Police during a review of system requirements. Any changes in

the proposed system or equipment will require a change order, which may incur additional costs.

1.1.1 Project Kick-off Meeting

The project kick-off meeting is scheduled as soon as possible following receipt of the contract. One of the main objectives of the meeting is to ensure that all project participants begin the project with a clear and shared understanding of the project and project expectations. During this meeting:

- A. Process owners are identified
- B. Key project milestones and objectives are introduced and discussed
- C. Review the overall project “As Purchased” design and Statement of Work (SOW).
- D. First review of the draft project plan

1.1.2 Project Workflow and Design Review Meeting

The purpose of the Call Flow and Design Review (CDR) meeting is to obtain a comprehensive understanding of your current operational environment and desired future workflow through interactive discussions. It is also to assist in understanding how the new VESTA 9-1-1 system can be configured to meet the operational needs.

- A. The Contractor will schedule project call flow and design review meetings with the MSP Program Manager. These meeting will be held at the site.
 - 1. The MSP Program Manager will ensure that key operational decision makers participate in these design meetings.
- B. During these meetings, The Contractor will gather critical information from MSP to set up and program the VESTA 9-1-1 system, including detailed review of trunks, lines and circuits. Motorola Solutions will work with you to document the final system design elements that will be used for all aspects of the programming and configuration of your VESTA 9-1-1 system. Design discussions and decisions will include but are not limited to:
 - 1. Detailed review of the “As Purchased” system design
 - 2. Detailed review of call flow and system design
 - 3. Detail review of Network Requirements
 - 4. Detail review of Network Components (routers and switches)
 - 5. Detailed review of the project Roles and Responsibilities of the collective team
 - 6. Site walks for Environmental Review & Intra-system interfaces
 - a. Environmental:

- 1) Power: outlets, power draw, UPS, generator
- 2) Cabling: positions, training room, backroom
- b. Adjuncts:
 - 1) CAD: ALI spill to CAD
 - 2) Recorder
 - 3) Mapping
 - 4) PBX
- c. Physical space, furniture, & logistics
- d. External interfaces: door access, alarms

It is critical that the State and the Contractor understand the responsibilities of each entity in this process. The detailed discovery and full disclosure of all facets of the Call Flow (how the different types of trunks, lines and circuits that are answered at the PSAP locations are routed to and answered by the current communications systems) and the Work Flow (how Call Takers and Dispatchers interact with callers and each other) is critical in the design of the new system. This will ensure a smooth and comprehensive transition.

1.1.3 Project Plan Approval

Once the system design has been finalized, the Contractors Program Manager will schedule resources for site implementation.

- A. The Contractor's resources will be scheduled, and dates communicated to the team members via the Motorola Solutions Project Schedule.
- B. The Motorola Solutions Schedule will be drafted and forwarded to MSP team members for review and comment.
 1. This "First Pass" schedule will be used to present MSP with the initial deployment schedule.
 2. Once all feedback and changes have been received and integrated into the schedule, the Master Project Schedule will be created and communicated by Motorola Solutions.
 3. Once published and a baseline established, the Master Schedule will only be changed as per appropriately submitted change requests.
- C. The Planning Phase ends when:
 1. The Project Plan has been approved
 2. System design and Call Flow are complete
 3. The Master Project Schedule has been developed and a consensus among concerned parties reached regarding deliverables and milestones

4. A draft site cut plan has been developed
5. A draft Acceptance Test Plan has been developed
6. The materials purchased from Motorola Solutions ship to the site

1.2 Phase II – Installation and Testing

Phase II is the period of time in which site preparation, site installation and testing take place. The project's implementation is accomplished to the degree that is possible without actually going "live", while minimizing disruption of the site's ongoing operations.

- A. The Contractor's Program Manager will coordinate the Phase II activities with the State's Program Manager to minimize interference with other site activities, while ensuring that the implementation and testing are completed as per the Project Plan and the Master Project Schedule.
- B. Implementation and Testing milestones and deliverables will be documented and managed via the Master Project Schedule.
- C. During this phase the components of the solution, including applications, servers, network components and data flow, are configured and readied for deployment. All network, regional and premise components are delivered, and the equipment rooms and other facilities are made ready.

1.2.1 Solution Staging

- A. The process starts with the staging of the system equipment at the Contractor's location.
 1. MSP site equipment will be assembled, configured, and burned in with MSP's specific site information, including but not limited to, system software, IP addresses, machine names, and line and trunk data.
 2. The equipment will be quality-checked for any defects or errors, then packaged and shipped to the MSP site for inventory and installation.

1.2.2 Site Installation

The Contractor will perform the following general steps for the system installation. Additional detail and steps will be added during project meetings. The Contractor will:

- A. Unpack and inventory equipment
- B. Uninstall and move old equipment and placed in a designated areas at each locations (The Contractor will not remove old equipment from the premise for disposal)
- C. Place/Install racks/cabinet

D. If new cabling is required:

1. Run cable from Contractor provided Connector Blocks to backboard for all 9-1-1 trunks
2. Run cable from Contractor provided Connector Blocks to backboard for all administrative lines
3. Run LAN cables from the Contractor provided rack/cabinet to all Contractor provided workstations; this includes providing an adequate number of cable runs for the voice/network, logging recorder, and any other equipment that may be required
4. Run LAN cables from any IP phones to the Contractor provided rack (if applicable)
 - a. Physical installation of all new VESTA 9-1-1 servers and associated components at the identified backrooms (Host A & B)
 - b. Physical installation of any network equipment required: switches, routers, etc. and associated cabling provided by the Contractor
 - c. Physical installation of all new peripheral devices at all sites
 - d. For each site, configure and make operable the system as documented in the Detail Design Document to include:
 - 1) Configure all new VESTA 9-1-1 system servers.
 - 2) Configure all new workstations purchased for the sites
 - 3) Perform Router Configuration
 - 4) Perform Firewall Configuration
 - e. Manage all appropriate data and accounts for the VESTA 9-1-1 system
 - f. Perform installation and configuration of the Contractor's provided MIS solution.

1.2.3 Testing

Testing is one of the major aspects of your VESTA 9-1-1 project and its success will require combined concentrated effort by MSP staff and the Contractor's staff.

- A. Upon execution of the Change Notice adding this work, the Contractor's Project Manager will work closely with the MSP Program Manger to review the System Acceptance Test Plan and make mutual agreed upon changes to the Test Plan.
 1. At the completion of the implementation, the State's designated participants and the Contractor will execute the test plan that displays the system is functioning and configured as designed and document test results.

- B. The Contractor will perform the various required tests using the agency's actual infrastructure, which is beneficial for the following reasons:
 - 1. Testing will be performed on the production solution – actual hardware
 - 2. Testing will be performed in the actual environment
 - 3. Testing will allow you to easily observe the process

1.2.4 Lockdown

The Implementation and Testing Phase ends when Site Implementation is complete and the site testing has been completed to the degree agreed upon during the project planning process.

- A. At the conclusion of the site's implementation and testing, a lockdown (configuration freeze) period will begin and remain in effect until system cutover.
- B. During implementation and training, vendors/providers of each subsystem will have the opportunity to perform pre-approved nominal system testing without making any user application and configuration changes.
- C. The site lockdown will be scheduled via the Master Project Schedule.

1.2.5 The State's Responsibilities During Installation

The State's responsibilities shall include, but are not limited to:

- A. Remove and dispose of all old equipment and peripheral at each locations
- B. Use reasonable efforts to provide supporting information to aid in the solution of any problems discovered during installation, implementation, or post installation phases of this project
- C. Provide appropriate schedule notification and facility availability for VESTA 9-1-1 on-site services and training
- D. Notify and coordinate schedule changes with Motorola Solutions, which may require a Change Order (and potentially additional charges) dependent upon the change
- E. Assume sole responsibility for the accuracy and completeness of Customer-supplied data
- F. Provide dedicated (2) 20A 110V Uninterrupted Power Supply (UPS) protected power outlets for the facilities and appropriate grounding, or as determined by the site survey, for the proper operation of the emergency telephone and computer systems described herein
- G. Provide required (2) Layer 2 Wide Area Network (WAN) connections for a Geo-diverse deployment between Host A and Host B. The Layer 2 bridged and

transparent transport connections will terminate on Ethernet RJ-45 ports or Single Form-factor Pluggable (SFP) as applicable if Dark Fiber is used, on the core Vesta Cisco switches. Two transport circuits riding alternate routes for redundancy and survivability are required.

- H. Ensure WAN links adheres to specifications detailed in the Motorola IP Networking Guide as well as the Motorola Solutions Bandwidth Estimate.
- I. Provide a floor plan outlining where the Contractor provided equipment is to be installed and position numbers for Call Taker, Dispatch, and Supervisor positions
- J. Ensure the operating environment is fully functional and meets VESTA 9-1-1 minimum operating requirements
- K. Provide the applicable broadband service for the VESTA 9-1-1 Virtual Private Network (VPN) for remote monitoring, support and troubleshooting connectivity
- L. Provide for, move, test, and make operational or otherwise deliver Centralized Automated Message Accounting (CAMA) trunks, administrative lines and other Public Switched Telephone Network (PSTN) connections to the backboard demarcation at least 14 days prior to installation start date
- M. Provide for, move, test, and make operational or otherwise deliver two (2) Automatic Location Identification (ALI) circuit connections to the backboard demarcation at least 14 days prior to installation start date
- N. Provide facility specific work and activity, including, but not limited to, construction, core drilling, grounding, and any electrical or conduit needed to support the implementation
- O. Assist Motorola Solutions in securing any required security clearances, identification tags and other requirements for access to areas within the facility necessary for Motorola Solutions personnel to complete their project responsibilities under this agreement
- P. Provide the tap to the network clock, if applicable. This includes all interfaces necessary, preferably to provide the name/address of a timeserver on the network.
- Q. Document and supply configuration information on the existing CPE
- R. Make available at the equipment rack, all remote access lines terminated on RJ 11 or RJ 45 jacks or contract with Motorola Solutions as required
- S. Ensure that or contract with Motorola Solutions to guarantee Intermediate Distribution Frame (IDF), wall boards and/or interconnect points appear in the immediate area where VESTA 9-1-1 servers are installed
- T. Provide/Reuse existing monitors are all locations

- U. Provide required adaptors for Monitors to connection proper to the Motorola provided Workstations
- V. Call Detail Record (CDR) Printers at all locations (if required)
- W. Administrative Printers at all locations (if required)
- X. Cabinet/Rack enclosure for the Detroit and Gaylord remote locations
- Y. Headsets for all Call Takers
- Z. Backroom UPS for all locations
- AA. ALI Modems (If applicable)
- BB. Keyboard, Video, Mouse switch (KVM's) (If applicable)
- CC. Telecommunications Center (TCC) Provider and Network charges

1.3 Phase III – Cutover

Cutover is the primary focus of this project, its success will require a methodical focus on planning, executing, and monitoring. The Draft Cutover Plan will specify specific tasks and responsibilities for the Contractor provided systems, materials, and services.

- A. The cutover plan includes the fallback process to restore the system to the pre-migration operation in the event of a catastrophic failure.
- B. The Cutover Plan defines the sequenced procedures and steps that will occur in the Cutover Phase to bring new equipment to an operational state, as well to transition services from the current equipment to the new. Appropriate safeguards are built in to ensure a cutover with minimal operational impact.
- C. The Cutover Phase is the major transition point for the project. The Contractor provided systems are brought online and site's operations shift from the old equipment to the new equipment. The Contractor's Program Manager will work with the MSP team to minimize the disruption for each Public-Safety Answering Point (PSAP). To that end, during the Planning Phase the decision will be made for the cutover plan. Examples of cutover options are as follows:
 - 1. Flash Cut: A flash cut requires a coordinated migration of 9-1-1 traffic to the PSAPs. Workstations at a site are cut over to the NG9-1-1. The benefit of a flash cut is that the PSAP personnel do not require temporary relocation to another PSAP that might not have the same radio or Computer Aided Dispatch (CAD) system, resulting in less disruption.
 - 2. Relocation Cut: You may choose to vacate their PSAP and operate at the alternate PSAP while their PSAP is upgraded. Once the upgrade is finished the personnel would systematically move to the new VESTA 9-1-1 system

D. The Cutover Phase will be scheduled via the Master Project Schedule.

1.3.1 The Contractor's Responsibilities During Cutover

The Contractor's Program Manager will coordinate assignment of appropriate Contractor's technical staff to support the transition to the new VESTA 9-1-1 system. Resource assignments will be planned and tracked via the Contractor's Project Schedule. The Contractor's responsibilities include:

- A. Pre-cut and Post-cut site testing which will be performed in accordance with the Contractor's System Acceptance Test Plan that will be provided based on the type of system(s) purchased
- B. The Contractors Program Manager will track Contractor Solutions issues and/ or exceptions noted during the site cutover and report updates to your team for updates to the Issues Control Log
- C. The Cutover Phase will end when the MSP project team agrees that all cutover objectives have been met

At the conclusion of the Cutover Phase, a meeting will be held with the project team members to discuss the cutover, any remaining Contractor issues, and to review the Post-Cutover Support Plan.

1.3.2 Customer Responsibilities During Cutover

The State will be responsible for the following during cutover:

- A. Schedule appropriate personnel to support the cutover
- B. Assume responsibility for cutover activities that are beyond the scope of the Contractor's deliverables as delineated in the approved Project Plan
- C. Coordinate third party services and/or activities during the cutover that are not part of the Contractor's deliverables but may affect systems and/ or services. This includes, but is not limited to Telco's, third party vendors, or other organizations that are participating in the cutover

1.4 Phase IV – Project Closure

Once all sites are operational and the post-cutover coverage is complete, the Project will move to closure phase. The project closure phase is the process of completing any open issues associated with the deployment of your project and to transition the project from Implementation to Support.

The Contractor's Project Manager will ensure all issues have been resolved or assigned for resolution. Any open issues at time of closure are to be transitioned to the Contractor's Technical Support, Site Installation, and Verification Package.

Project closure will occur when:

- A. All sites have cutover to the new VESTA 9-1-1 systems
- B. All on-site post cutover support has been completed
- C. All System Acceptance Testing has been successfully executed and approved by Michigan State Police
- D. MSP has signed the Site Acceptance document

1.4.1 Site Installation and Verification Package

The Contractor will provide “as-built” documentation:

- A. CPE inventory, including a complete list of installed equipment
- B. Solution Overview / Detailed System Document
- C. System Diagrams
- D. IP Schema and Naming Convention
- E. Bandwidth Estimates
- F. System Acceptance Test
- G. Other documentation as mutually agreed to by the parties

1.5 Phase V – System Warranty and Maintenance

The Contractor’s onsite response system warranty and maintenance service will be provided to the State as needed. Certified and trained technicians will perform diagnostics, remove components for repair and reinstall new or reconditioned components.

1.5.1 VESTA 9-1-1 Operations Manager (ECH Service Management)

A VESTA 9-1-1 Operations Manager will be assigned to provide the State with a field-based single point of contact and manage the contracted maintenance and support services.

- A. The Operations Manager works with the on-site support personnel and is backed by the Contractors service and support organization.
 - 1. This support organization includes the Network Security Operations Center (NOC), Technical Support, and product management teams (as required). All work in concert with on-site support personnel to deliver services and maintain Service Level Agreements.
- B. The Operations Manager assigned for this Statement of Work is identified as:

Operation Manager's Name- **TBD** (and provided to the Agency Program Manager)
Email Address
Phone number

C. The Operations Manager will do the following:

1. Create and maintain the Support Plan.
2. Establish and refine policies and procedures to consistently maximize service performance.
3. Proactively manage the life cycle of the service and supply information regarding upgrades and updates.
4. Engage the appropriate resources, teams, and individuals to troubleshoot and resolve complex service issues.
5. Serve as the escalation point of contact when standard troubleshooting efforts are unsuccessful.
6. Serve as the liaison to Motorola's support organization for escalated incidents.
7. Provide timely and frequent informational updates about progress towards resolving incidents.
8. Maintain the service and performance quality of the system.
9. Monitor Motorola's contractual support and provide reviews and analyses of the support performance.
10. Manage the Change Management process during the Service operation

1.5.2. Network Security and Operation Center (NSOC)

Designed exclusively for Public Safety communications, the NSOC includes state-of-the-art technology, processes and tools all provided by our highly trained, dedicated team. With connectivity to the NSOC, our advanced systems facilitate true Emergency Services-grade monitoring and management.

1.5.2.1. Service Desk

The Service Desk is the central point of contact to report incidents and submit change requests. Co-located with the Technical Support Center within the Network and Security Operations Center (NSOC), the Service Desk maintains a holistic view of your service delivery environment. The Service Desk will:

- A. Open a case and categorize the reported issue or request
- B. Resolve incidents based on priority

- C. Perform analysis to assist in identifying a corrective action plan
- D. Escalate the incident/request to technical or service experts when required
- E. Engage the next level management to ensure timely problem resolution, when necessary
- F. Provide regular status updates for escalated incidents

1.5.2.2. Monitor and Response

With this service system thresholds, established during the Monitoring and Response service implementation, are continually monitored by the system.

- A. Anytime the system performance exceeds the threshold limit, Monitoring and Response is immediately notified via digital alarm.
- B. The Contractor then notifies the designated maintenance provider (to be determined at the time the system is ordered or at the kick-off meeting) via the means (email, phone, etc.) set up upon implementation. This is a very stringent process that takes place in seconds.
- C. Monitoring and Response will provide pre-failure hardware notification, and generate alerts on service/device state changes, runaway processes, and memory leaks. It will collect and store user- defined performance counters, and stores event log messages, performance data, and configuration data in a centralized database. Below are some of the features available through Monitoring and Response:
 - 1. Proactively monitors key systems to detect faults and mitigate risks to ensure highest possible system performance and availability
 - 2. Monitors each server, workstation and networking device for hardware alarms, software alarms and performance thresholds
 - 3. Minimizes risk and the possibility of service interruptions, predicting issues before they occur
 - 4. Alarms the NSOC for remediation, notification and escalation, with most alarms resolved remotely

1.5.2.3 Anti-Virus

- A. The Contractor will provide anti-virus protection as a service, ensuring updates are tested and applied in a timely, efficient manner
- B. The antivirus solution will be certified for our call handling platforms and continuously updated to automatically detect and remove the latest viruses.

1.5.2.4 Patch Management

Patch Management will deploy Microsoft® updates and patches after validating they are compatible with your solution. This will help ensure system integrity and security, especially when bundled with Virus Protection for comprehensive, hands-free care

4.2.3.5 Software Upgrades

The Contractor's Operation Manager, working with MSP's Program Manager and staff, will oversee all approved hardware and software upgrades.

- A. The Contractor will provide the customer notification of scheduled product updates and/or modifications via a Product Change Notice (PCN) or a Product Bulletin (PB).
- B. The State will ensure that their software or firmware release complies with the lifecycle milestones as defined in the Support Program as follows:
 1. **End of Sales (EOS)** occurs 12 months after the date that a new version is made generally available (GA). Previous version of software are not available in new systems. Bug fixes are supported and license add-ons are available
 2. **End of Expansion Sales (EOES)** occurs 12 months after EOS. No upgrades, spares, or add-on for the previous version of software are available upon End of Life (EOL). Bug fixes are not available
 3. **End of Support Date (EOSD)** occurs 12 months from EOES. This is the last date to receive support for the software version. Motorola Solutions will try to resolve any issues beyond that given date
 4. **Custom Extended Support (CES)** is available for 24 months from the EOSD. CES provided continued access to Technical Support past the EOSD period. Motorola Solutions will try to resolve any issues beyond the given date. Dates and product release versions for each milestone are published here, [VESTA 9-1-1 Emergency Call Handling Products Software Lifecycle Matrix](#)

Added via CN #7, Effective 9/1/2023

MA # 190000001554

STATE OF MICHIGAN

**Michigan's Public Safety Communication System (PMSCS) Continued System Updates, Equipment Maintenance and Updates, and Ancilliary Systems Products
SCHEDULE B.2. - PRICING- MSP**

COMPONENT		10/1/2019	10/1/2020	10/1/2021	10/1/2022	10/1/2023	10/1/2024	10/1/2025	10/1/2026	10/1/2027	10/1/2028	TOTAL
MSP	Vesta 9-1-1					\$ 1,575,004.00						\$ 1,575,004.00
	Vesta 9-1-1 Annual Warranty and Maintenance	-	-	-	-		\$ 174,284.00	\$ 181,256.00	\$ 188,506.00	\$ 196,046.00		\$ 740,092.00
	TOTAL					\$ 1,575,004.00	\$ 174,284.00	\$ 181,256.00	\$ 188,506.00	\$ 196,046.00		\$ 2,315,096.00

Pricing Notes:

Vesta 9-1-1 is based on Schedule L, Phases 1 through 4, and the Equipment List for two host and two remote locations as listed in Contractor's quote dated June 14, 2023 Sections 7.1, 7.2, 7.3 and 7.4
 Vesta 9-1-1- Warranty and Maintenance is based on Schedule L, Phase 5



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 320 S. WALNUT ST., LANSING, MICHIGAN 48933
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **5**
 to
 Contract Number **190000001544**

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago, IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Kate Jannereth	DTMB
		517-881-1031	
	jannerethk@Michigan.gov		
	Contract Administrator	Valerie Hiltz	DTMB
(517) 249-0459			
hiltzv@michigan.gov			

CONTRACT SUMMARY

MPSCS CONTINUED SYSTEM UPDATES, EQUIPMENT, MAINTENANCE AND UPGRADES, AND ANCILLARY SYSTEMS PRODUCTS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
October 1, 2019	December 31, 2029	0 - 0 Year	December 31, 2029
PAYMENT TERMS		DELIVERY TIMEFRAME	
NET 45		As per Delivery Order	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

As per delivery order.

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		December 31, 2029
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$99,900,000.00	\$0.00	\$99,900,000.00		

DESCRIPTION

Effective October 1, 2022 this contract is revising language, as attached, in Attachment 1 to Schedule A, by adding specifications surrounding an Astro System Manager and is revising Schedule B, as attached, to include True Up for the addition of 20 new entities on the system, the additional four year agreement for Lab as a Service, and the cost of the Astro 25 System Manager.

All other terms, conditions, specifications and pricing remain the same per Contractor and MPSCS agreement and DTMB Central Procurement Services approval.

The following language is added to Attachment 1 to Schedule A, Astro 25 System Upgrade Agreement II (SUA II)

1.18 MPSCS ASTRO System Manager

The Contractor will provide to the State a System Manager who will be responsible for the following:

- 1.18.1 Expected to be on site for meetings with customer as needed
- 1.18.2 Engage with the customer regularly as required to keep an open communication plan with the NCC and their management team.
- 1.18.2 Track all technical support cases until resolution. Escalate cases as necessary, working directly within the TS organization. This may also include cases regarding SUS, LXP, etc.
- 1.18.3 Address any perceived or actual product quality issue by opening a case and perusing it to resolution. This may include facilitating conversations between MPSCS stakeholders and MSI subject matter experts.
- 1.18.4 Address any concern or issues the customer may bring to you and work to resolution.
- 1.18.5 Recognize maintenance issue trends and plan for/ propose upgrade corrective actions.
- 1.18.6 Attend any conference calls or meetings invited to in relation to any MPSCS proposal or integration project.
- 1.18.7 Actively participate in the Tier 1 DDP creation and review process.
- 1.18.8 Review and advise customer on all ASTRO MTNs. Assist in implementation if necessary.
- 1.18.9 Participate in applicable system ATPs
- 1.18.10 Track and reconcile ASTRO and other system licenses as sold to MPSCS by MSI.
- 1.18.11 Actively participate in SUA discussions and in onsite system upgrade activities.
- 1.18.12 Create and track system matrix.
- 1.18.13 Act as liaison between customer and Motorola product groups to help the NCC and engineering teams to discuss existing and new features.
- 1.18.14 Coordinate TNCT for customer configurations (firewall rules, critical connect, etc)
- 1.18.15 Coordinate the NCC Project Tracker activities with BGA as required

STATE OF MICHIGAN

Michigan's Public Safety Communication System (PMSCS) Continued System Updates, Equipment Maintenance and Updates, and Ancilliary Systems Products

SCHEDULE B- PRICING

COMPONENT		10/1/2019	10/1/2020	10/1/2021	10/1/2022	10/1/2023	10/1/2024	10/1/2025	10/1/2026	10/1/2027	10/1/2028	TOTAL
MPSCS ASTRO LIFECYCLE	System Upgrade Agreement II (SUA II)	\$ 4,666,781.89	\$ 5,119,186.80	\$ 5,570,726.31	\$ 5,900,187.68	\$ 6,460,906.70	\$ 6,502,411.06	\$ 6,545,043.90	\$ 6,589,066.01	\$ 6,634,415.11	\$ 6,681,002.78	\$ 60,669,728.24
	Security Update Services (SUS)	\$ 100,785.87	\$ 103,809.45	\$ 106,923.73	\$ 118,189.84	\$ 121,735.54	\$ 125,387.60	\$ 135,019.65	\$ 139,070.24	\$ 143,242.35	\$ 147,539.62	\$ 1,241,703.89
	Technical Support (TS)	\$ 252,878.41	\$ 260,464.76	\$ 268,278.70	\$ 296,546.12	\$ 305,442.50	\$ 314,605.77	\$ 338,773.22	\$ 348,936.41	\$ 359,404.51	\$ 370,186.64	\$ 3,115,517.04
	OPSOC	\$ 34,839.75	\$ 35,884.94	\$ 36,961.49	\$ 40,855.97	\$ 42,081.65	\$ 43,344.10	\$ 46,673.71	\$ 48,073.92	\$ 49,516.14	\$ 51,001.63	\$ 429,233.30
	Busines Relationship Manger (BRM)	\$ 260,000.00	\$ 267,800.00	\$ 275,834.00	\$ 284,109.02	\$ 292,632.29	\$ 301,411.26	\$ 310,453.60	\$ 319,767.21	\$ 329,360.22	\$ 339,241.03	\$ 2,980,608.63
TOTAL	\$ 5,315,285.92	\$ 5,787,145.95	\$ 6,258,724.23	\$ 6,639,888.63	\$ 7,222,798.68	\$ 7,287,159.79	\$ 7,375,964.08	\$ 7,444,913.79	\$ 7,515,938.33	\$ 7,588,971.70	\$ 7,588,971.70	\$ 68,436,791.10
TRUE UP	True Up 10-01-21 to 09-30-29 integrations			\$ 78,583.61	\$ 468,078.64	\$ 686,602.80	\$ 705,746.39	\$ 725,535.98	\$ 745,917.17	\$ 766,904.45	\$ 788,517.97	\$ 4,965,887.01
TRUE UP	True Up 10-01-22 to 09-30-29 integrations					\$ 103,591.78	\$ 571,378.84	\$ 589,948.65	\$ 607,647.11	\$ 625,876.52	\$ 644,652.82	\$ 3,143,095.72
CRITICAL CONNECT	Critical Connect			\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 760,320.00
	Astro Connectivity Managed Service			\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 458,400.00
	System Upgrade Agreement II (SUA II)				\$ 35,596.00	\$ 36,664.00	\$ 37,764.00	\$ 38,897.00	\$ 40,064.00	\$ 41,266.00	\$ 42,503.00	\$ 272,754.00
	Security Update Services (SUS)				Included	Included	Included	Included	Included	Included	Included	Included
TOTAL			\$ 152,340.00	\$ 187,936.00	\$ 189,004.00	\$ 190,104.00	\$ 191,237.00	\$ 192,404.00	\$ 193,606.00	\$ 194,843.00	\$ 194,843.00	\$ 1,491,474.00
MPSCS PREMIER**	PremierOne CAD		\$ 106,678.14	\$ 109,878.36	\$ 119,812.29	\$ 123,406.92	\$ 127,108.85	\$ 135,644.68	\$ 139,714.22	\$ 143,905.79	\$ 148,222.50	\$ 1,154,371.75
	PremierMDC	\$ 162,778.86	\$ 150,358.48	\$ 154,869.30	\$ 171,187.28	\$ 176,322.96	\$ 181,612.64	\$ 195,563.48	\$ 201,430.32	\$ 207,472.88	\$ 213,696.68	\$ 1,815,292.88
	Upgrade- Hardware / Software / Services		\$ 142,848.92	\$ 142,848.92	\$ 153,301.28	\$ 153,301.28	\$ 153,301.28	\$ 160,269.52	\$ 160,269.52	\$ 160,269.52	\$ 160,269.52	\$ 1,386,679.76
TOTAL	\$ 162,778.86	\$ 399,885.54	\$ 407,596.58	\$ 444,300.85	\$ 453,031.16	\$ 462,022.77	\$ 491,477.68	\$ 501,414.06	\$ 511,648.19	\$ 522,188.70	\$ 522,188.70	\$ 4,356,344.39
OTHER ADD ONS	Lab as a Service (Five Year Agreement)		\$ 655,000.00	\$ 674,650.00	\$ 694,890.00	\$ 715,736.00	\$ 737,208.00					\$ 3,477,484.00
	Lab as a Service (Four Year Agreement)							\$ 761,167.26	\$ 785,905.20	\$ 811,447.11	\$ 837,819.15	\$ 3,196,338.72
	CommandCenter Aware				\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 143,486.00
	Learning Subscription Astro/Cyber					\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 142,653.00
	Astro 25 System Manager				\$ 208,333.33	\$ 258,125.00	\$ 266,514.06	\$ 275,175.77	\$ 284,118.98	\$ 293,352.85	\$ 302,886.82	\$ 1,888,506.81
TOTAL		\$ 655,000.00	\$ 674,650.00	\$ 923,721.33	\$ 1,018,134.50	\$ 1,047,995.56	\$ 1,080,616.53	\$ 1,114,297.68	\$ 1,149,073.46	\$ 1,184,979.47	\$ 1,184,979.47	\$ 8,848,468.53
GRAND TOTALS		\$ 5,478,064.78	\$ 6,842,031.49	\$ 7,571,894.42	\$ 8,663,925.45	\$ 9,569,571.14	\$ 9,693,028.51	\$ 9,864,831.27	\$ 9,998,946.70	\$ 10,137,170.43	\$ 10,279,500.84	\$ 91,242,060.75



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 320 S. WALNUT ST., LANSING, MICHIGAN 48933
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **4**
 to
 Contract Number **190000001544**

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago, IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Kate Jannereth	DTMB
		517-881-1031	
		jannerethk@Michigan.gov	
	Contract Administrator	Valerie Hiltz	DTMB
		(517) 249-0459	
		hiltzv@michigan.gov	

CONTRACT SUMMARY

MPSCS CONTINUED SYSTEM UPDATES, EQUIPMENT, MAINTENANCE AND UPGRADES, AND ANCILLARY SYSTEMS PRODUCTS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
October 1, 2019	December 31, 2029	0 - 0 Year	December 31, 2029
PAYMENT TERMS		DELIVERY TIMEFRAME	
NET 45		As per Delivery Order	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

N/A

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		December 31, 2029
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$99,900,000.00	\$0.00	\$99,900,000.00		

DESCRIPTION

Effective August 1, 2022 this contract is adding Schedule K- Critical Connect/ Wave PTX Engineering Services as attached.
 All other terms, conditions, specifications and pricing remain the same per Contractor and MPSCS agreement and DTBM Central Procurement Services approval.

Added Via CN #4, effective 8/1/2022

MA 190000001544

SCHEDULE K

MPSCS

Critical Connect / WAVE PTX Engineering Services Statement of Work (SOW)

A. Introduction

As part of the MPSCS Critical Connect - Core Enhancement program Motorola Solutions Inc. (Contractor) will provide Engineering Services, for a period of six (6) months with option to continue as needed on a monthly basis at the monthly rate listed on the pricing page. This Statement of Work (SOW) is an integral part of the Subscription Services Agreement for the Critical Connect and/or WAVE PTX Services entered into by Motorola Solutions and MPSCS (Customer) and will be governed by the terms and conditions in the Agreement. If there is a conflict between the terms of the Agreement and the terms of this SOW, the terms of the Master Agreement will govern.

B. Contractor Scope of work:

The Contractor will cover the following activities during the duration of the service:

1. The Contractor's engineering representative will attend meetings with the Contractor's Project Manager and the State to review the status of the action items, top ten issues, and ongoing Critical Connect and/or WAVE PTX projects. The Contractor will implement a workbook to track all the topics discussed during the meetings and action items.
2. The Contractor's engineering representative will attend the System Security Plan meetings with the State to review the System Security Plan document provided by the MPSCS and assist in building the Final System Security Plan based on the Customer's security requirements and Authority to Operate (ATO). Engage the Motorola Solutions' System Architects / Cyber Security / Development Team as required.
3. The Contractor's engineering representative will attend the WAVE PTX and Critical Connect On boarding Plan meetings with the State and jointly develop the WAVE PTX and Critical Connect On boarding Plans. Provide the documents and training to the MPSCS Admin group as required.
4. The Contractor's engineering representative will be the point of contact and communicate the status and progress of the Critical Connect / WAVE PTX deployment projects. Review Acceptance Test Plan (ATP) document with the Customer and perform ATP.
5. The Contractor's engineering representative will participate, collaborate and follow up major cases that affect Critical Connect /WAVE PTX service and/or State issues during normal business hours. The Contractor will

provide recommendations on the Critical Connect / WAVE PTX performance improvement based on the lessons learned.

6. The Contractor's engineering representative will work with the Contractor's field team and the State to and complete the deployment of the Critical Connect solution in the MPSCS LaaS environment and production system.
7. The Contractor's engineering representative will develop the WAVE 5K to WAVE PTX Subscriber Migration Plan and review with the State. Provision the target users and Talk groups as agreed. Coordinate the production cutover with the MPSCS staff. After the soak period mutually agreed with the Customer, decommission the WAVE 5K System.
8. The Contractor's engineering representative will develop the Critical Connect Subscriber Migration Plan and review with the State. Provision the target users and Talk groups as agreed. Coordinate the production cutover with the MPSCS staff.
9. The Contractor's engineering representative will develop, coordinate and deliver training on WAVE PTX and Critical Connect for the NCC, Business Unit and other impacted areas on processes, functionality and on boarding.
10. The Contractor's engineering representative will be the point of contact for Patching Portal. Document processes; work with MPSCS on setup, security and access controls. Train MPSCS and dispatch personnel on Patching Portal. Develop Roles and Responsibilities of all support personnel.
11. The Contractor's engineering representative will participate and document results of tabletop exercises in order to work through on boarding and process issues for Wave PTX and Critical Connect.

C. General:

1. The State will provide all necessary access to information, personnel and/or documentations as required for Motorola Solutions to provide this service. This includes providing the System Security Plan document and participating in the meetings described above.
2. The State will provide the facilities at the Customer office for the Contractor's engineer when he/she is on site. The solutions engineer will be on site once a month, flying in on Monday and flying out the Friday of the same week.
3. The State will participate and witness ATP, and sign the ATP document upon successful ATP.
4. The State will purchase the licenses as required for W5K User migration.

5. This service will be provided during normal business hours according to the USA, the State's, and the Contractor's scheduled holidays.
6. In the event of Critical Connect / WAVE PTX service outage, the State will contact the Customer through the Motorola Solutions service desk, provide all necessary information, open a ticket and collaborate with WAVE/Critical Connect support team to troubleshoot/investigate. The Contractor's engineer assigned by this service is not the 1st line of the contact; he/she may participate in troubleshooting activities during normal business hours as required.
7. The Contractor's engineering representative will help the NCC with initial troubleshooting and training as they learn what Wave PTX (if applicable) and Critical Connect will look like from their point of view. Document how to determine between a fiber cut/LTE outage/MPSCS issue.

D. Pricing

PRICING TOTALS	
Professional Services: Critical Connect / WAVE PTX Engineering services for six (6) months (See option pricing below for additional months) Product Code: SI128AH APC: 639	\$125,000.00
Cost per month to extend beyond the initial six (6) month period	\$20,834.00

E. Payment

See Standard Contract Terms, Section 24. Terms of Payment and Schedule A, Section 8.2. Payment Methods.



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **3**
 to
 Contract Number **190000001544**

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago, IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Kate Jannereth	DTMB
		517-881-1031	
	jannerethk@Michigan.gov		
	Contract Administrator	Valerie Hiltz	DTMB
(517) 249-0459			
hiltzv@michigan.gov			

CONTRACT SUMMARY

MPSCS CONTINUED SYSTEM UPDATES, EQUIPMENT, MAINTENANCE AND UPGRADES, AND ANCILLARY SYSTEMS PRODUCTS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
October 1, 2019	December 31, 2029	0 - 0 Year	December 31, 2029
PAYMENT TERMS		DELIVERY TIMEFRAME	
NET 45		As per Delivery Order	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

N/A

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		December 31, 2029
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$99,900,000.00	\$0.00	\$99,900,000.00		

DESCRIPTION

Effective March 25, 2022 this contract is adding Schedule I- Learning Subscription and Schedule J- Central Command Aware Plus, and is revising Schedule B- Pricing as attached.

All other terms, conditions, specifications and pricing remain the same, per Contractor and MPSCS agreement and DTMB Central Procurement Services approval.

STATE OF MICHIGAN

Michigan's Public Safety Communication System (PMSCS) Continued System Updates, Equipment Maintenance and Updates, and Ancillary Systems Products

SCHEDULE B- PRICING

	COMPONENT	10/1/2019	10/1/2020	10/1/2021	10/1/2022	10/1/2023	10/1/2024	10/1/2025	10/1/2026	10/1/2027	10/1/2028	TOTAL
MPSCS ASTRO LIFECYCLE	System Upgrade Agreemnt II (SUA II)	\$ 4,666,781.89	\$ 5,119,186.80	\$ 5,570,726.31	\$ 5,900,187.68	\$ 6,460,906.70	\$ 6,502,411.06	\$ 6,545,043.90	\$ 6,589,066.01	\$ 6,634,415.11	\$ 6,681,002.78	\$ 60,669,728.24
	Security Update Services (SUS)	\$ 100,785.87	\$ 103,809.45	\$ 106,923.73	\$ 118,189.84	\$ 121,735.54	\$ 125,387.60	\$ 135,019.65	\$ 139,070.24	\$ 143,242.35	\$ 147,539.62	\$ 1,241,703.89
	Technical Support (TS)	\$ 252,878.41	\$ 260,464.76	\$ 268,278.70	\$ 296,546.12	\$ 305,442.50	\$ 314,605.77	\$ 338,773.22	\$ 348,936.41	\$ 359,404.51	\$ 370,186.64	\$ 3,115,517.04
	OPSOC	\$ 34,839.75	\$ 35,884.94	\$ 36,961.49	\$ 40,855.97	\$ 42,081.65	\$ 43,344.10	\$ 46,673.71	\$ 48,073.92	\$ 49,516.14	\$ 51,001.63	\$ 429,233.30
	Busines Relationship Manger (BRM)	\$ 260,000.00	\$ 267,800.00	\$ 275,834.00	\$ 284,109.02	\$ 292,632.29	\$ 301,411.26	\$ 310,453.60	\$ 319,767.21	\$ 329,360.22	\$ 339,241.03	\$ 2,980,608.63
	TOTAL	\$ 5,315,285.92	\$ 5,787,145.95	\$ 6,258,724.23	\$ 6,639,888.63	\$ 7,222,798.68	\$ 7,287,159.79	\$ 7,375,964.08	\$ 7,444,913.79	\$ 7,515,938.33	\$ 7,588,971.70	\$ 68,436,791.10
TRUE UP	True Up 10-01-21 to 09-30-29 integrations			\$ 78,583.61	\$ 468,078.64	\$ 686,602.80	\$ 705,746.39	\$ 725,535.98	\$ 745,917.17	\$ 766,904.45	\$ 788,517.97	\$ 4,965,887.01
CRITIAL CONNECT	Critical Connect			\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 95,040.00	\$ 760,320.00
	Astro Connectivity Managed Service			\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 57,300.00	\$ 458,400.00
	System Upgrade Agreement II (SUA II)				\$ 35,596.00	\$ 36,664.00	\$ 37,764.00	\$ 38,897.00	\$ 40,064.00	\$ 41,266.00	\$ 42,503.00	\$ 272,754.00
	Security Update Services (SUS)				Included	Included	Included	Included	Included	Included	Included	Included
	TOTAL			\$ 152,340.00	\$ 187,936.00	\$ 189,004.00	\$ 190,104.00	\$ 191,237.00	\$ 192,404.00	\$ 193,606.00	\$ 194,843.00	\$ 1,491,474.00
MPSCS PREMIER**	PremierOne CAD		\$ 106,678.14	\$ 109,878.36	\$ 119,812.29	\$ 123,406.92	\$ 127,108.85	\$ 135,644.68	\$ 139,714.22	\$ 143,905.79	\$ 148,222.50	\$ 1,154,371.75
	PremierMDC	\$ 162,778.86	\$ 150,358.48	\$ 154,869.30	\$ 171,187.28	\$ 176,322.96	\$ 181,612.64	\$ 195,563.48	\$ 201,430.32	\$ 207,472.88	\$ 213,696.68	\$ 1,815,292.88
	Upgrade- Hardware / Software / Services		\$ 142,848.92	\$ 142,848.92	\$ 153,301.28	\$ 153,301.28	\$ 153,301.28	\$ 160,269.52	\$ 160,269.52	\$ 160,269.52	\$ 160,269.52	\$ 1,386,679.76
	TOTAL	\$ 162,778.86	\$ 399,885.54	\$ 407,596.58	\$ 444,300.85	\$ 453,031.16	\$ 462,022.77	\$ 491,477.68	\$ 501,414.06	\$ 511,648.19	\$ 522,188.70	\$ 4,356,344.39
OTHER ADD ONS	Lab as a Service (Five Year Agreement)		\$ 655,000.00	\$ 674,650.00	\$ 694,890.00	\$ 715,736.00	\$ 737,208.00					\$ 3,477,484.00
	CommandCentral Aware				\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 20,498.00	\$ 143,486.00
	Learning Subscription Astro/Cyber					\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 23,775.50	\$ 142,653.00
	TOTAL		\$ 655,000.00	\$ 674,650.00	\$ 715,388.00	\$ 760,009.50	\$ 781,481.50	\$ 44,273.50	\$ 44,273.50	\$ 44,273.50	\$ 44,273.50	\$ 3,763,623.00
GRAND TOTALS		\$ 5,478,064.78	\$ 6,842,031.49	\$ 7,571,894.42	\$ 8,455,592.12	\$ 9,311,446.14	\$ 9,426,514.45	\$ 8,828,488.24	\$ 8,928,922.52	\$ 9,032,370.47	\$ 9,138,794.87	\$ 83,014,119.50

STATE OF MICHIGAN

SCHEDULE I- LEARNING SUBSCRIPTION

TABLE OF CONTENTS

- Training Plan..... 1-3
 - 1.1 Training Overview..... 1-3
 - 1.2 Motorola Solutions Training 1-3
 - 1.2.1 Training Delivery..... 1-4
 - 1.2.2 Training Courses 1-4
 - 1.2.3 Training Tools..... 1-5
 - 1.2.4 Custom Training Solution..... 1-5
 - 1.2.4.1 Learning Subscriptions..... 1-5
 - 1.2.4.2 Learning Subscription Features 1-5
 - 1.2.4.3 ASTRO Hub..... 1-6
 - 1.2.4.4 CYBERSECURITY Hub 1-6
 - 1.3 Proposed Training for Michigan - MPSCS 1-6
 - 1.3.1 Learning Subscription..... 1-6
 - 1.3.2 Training Qualifications and Assumptions 1-7
 - 1.4 Pricing Information 1-8
 - 1.5 Contact Information 1-8

TRAINING PLAN

1.1 TRAINING OVERVIEW

Partnering with Motorola Solutions will enable Michigan - MPSCS to build personnel competency and maximize return on investment.

Effective training ensures successful implementation and use of your communications system by all personnel for the life of the system. The training plan furnished to Michigan - MPSCS is comprised of targeted coursework developed and delivered by our expert instructors. This plan, included below, will effectively provide Michigan - MPSCS personnel with a comprehensive understanding of the proposed system and user equipment.



We will collaborate with Michigan - MPSCS to tailor a final training plan to enable Michigan - MPSCS organization to operate, configure, and manage the proposed solution effectively and efficiently.

1.2 MOTOROLA SOLUTIONS TRAINING

Motorola Solutions provides an expanding portfolio of training delivery methods, tools, and courses to support the training needs of our customers. The figure below shows the elements of our training methodology that qualify us as the leader in the communications training industry.

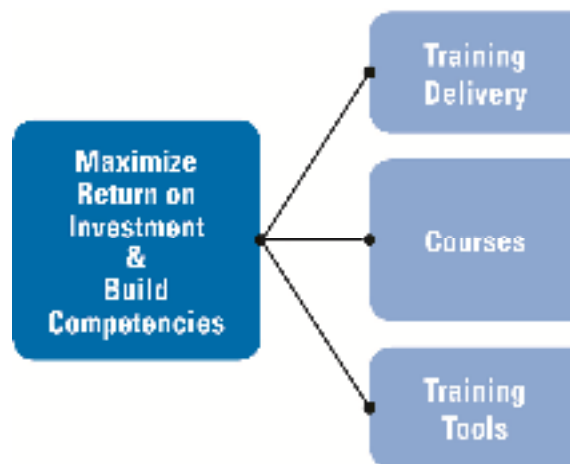


Figure 1-1: Build the competencies of Michigan - MPSCS personnel and maximize your return on investment with Motorola Solutions' expanding portfolio of training delivery methods, tools, and courses.

1.2.1 Training Delivery

Training Methods

Motorola Solutions' training experience and expertise enables our customers to gain the training they need to use during critical times in a variety of methods. As shown in the figure below, we offer three interactive methods of training: Online Self-Paced, Virtual Instructor-Led, and Instructor-Led.



Figure 1-2: Motorola Solutions offers a variety of interactive training methods that cater to different learning techniques, allowing more effective ways to give personnel the skills they need.

These training approaches ensure our customers receive the understanding they need for the practical aspects of their jobs.

1.2.2 Training Courses

Motorola Solutions offers a wide range of training courses to help our customers improve their proficiency and meet their designated outcomes.

Our specialized courses/curriculums are designed for our customers' role. Whether they are an administrator, technician or general user, Motorola Solutions makes sure our customers are equipped with foundational and advanced skills.

1.2.3 Training Tools

Tracking and Reporting

All customer training is tracked and student progress can be reported on. Our Learning Experience Portal (LXP) tracks and records all courses completed throughout the user experience.

1.2.4 Custom Training Solution

No two organizations have the same learning needs. Teams have unique requirements based on role, operational alignment, and technology. A one-size-fits-all approach can lead to misspent time and resources. The Motorola Solutions Learning Subscription is the solution for today's diverse teams and evolving technologies. It is designed to support on-demand learning that allows organizations to adapt to change - whether it's new technology or new reporting requirements. Your subscription can scale easily depending on need. Most importantly, users will have on-demand content that is personalized and easy-to-find. The outcome: less time wasted, more information when you need it most.

1.2.4.1 Learning Subscriptions

Learning Subscriptions are cloud-based and centrally-hosted, allowing each agency to scale the subscription to its own needs. Subscriptions are offered on a yearly basis and include unlimited access to self-paced online training for one preferred technology. Additional product technology hubs can easily be added as your needs evolve. Subscriptions include specific learning experiences based on your team's roles. Plus, our learning management platform allows you to quickly assign online or in-person training sessions and develop tailored curriculums, with deep tracking and reporting capabilities.

1.2.4.2 Learning Subscription Features

Motorola Solutions Learning Subscriptions empower your team with unique features:

- Unlimited online learning access to maximize your unique technology capabilities for demanding missions
- Learner focused content in multiple modalities to help keep pace with technological changes
- Role and task based curated training to develop new skills and deepen understanding of your technologies
- Discounted open registration classes at our Motorola Solutions Facilities
- Live virtual professor sessions to build expertise
- Track and report training progress to identify areas of improvement
- Synchronize learning with your solution's life cycle

1.2.4.3 ASTRO Hub

Learning Subscriptions offer unlimited access to the Motorola Solutions Learning eXperience Portal (LXP) and hands-on training for a deeper experiential learning environment. Through technology-specific hubs, essential documentation and tools are always current, and always available to meet your team's evolving learning needs. The ASTRO Hub includes access to online training and documentation for a wide variety of products, topics, roles, and skills.

1.2.4.4 CYBER Hub

Learning Subscriptions offer unlimited access to the Motorola Solutions Learning eXperience Portal (LXP) and hands-on training for a deeper experiential learning environment. Through technology-specific hubs, essential documentation and tools are always current, and always available to meet your team's evolving learning needs. The CYBER Hub includes access to online training and documentation for a wide variety of products, topics, roles, and skills.

1.3 PROPOSED TRAINING FOR MICHIGAN - MPSCS

1.3.1 Learning Subscription

Course Title	Target Audience	Sessions	Duration	Location	Date	Users
ASTRO Learning Subscription (All ASTRO Self-Paced Content Included)	General	Unlimited	7 Years	Self-paced; Online	N/A	101
CYBER Learning Subscription (All CYBER Self-Paced Content Included)	General	Unlimited	7 Years	Self-paced; Online	N/A	101

1.3.2 Training Assumptions and Qualifications

1. A successful training event requires that the students have adequate time for hands-on interaction with their equipment. The customer or project team will supply product equipment, cables, and test equipment. The Motorola Solutions Worldwide Education recommends that there be one subscriber unit available per participant in the training session. For console end user training, we recommend one console position for every two dispatch operators.
2. A successful training event also requires appropriate classroom environment in which to deliver training. The customer or project team will ensure that the necessary equipment (which includes a whiteboard, projector, student tables and chairs) is in place for the training event.
3. Electronic student materials will be furnished by Motorola Solutions Worldwide Education.
4. While it is important that Motorola Solutions meets the customer's requested training dates, the final class dates are determined by instructor availability. This is especially important when training in a language other than English because of the limited resources available.
5. Training dates will only be scheduled once payment has been received by the Motorola Solutions Worldwide Education. Without payment, Motorola Solutions reserves the right to cancel a field training course. By supplying the agreed form of payment, the Customer or project team accepts all terms and conditions.
6. Acknowledging there are costs associated with preparing a training program, the Customer agrees to notify the Motorola Solutions Worldwide Education immediately if Customer or project team requires a date change for a scheduled training event. If a class is cancelled or postponed within 30 days of the scheduled training, the Customer will pay 100% of the instructor delivery rate and any additional costs which have been incurred (i.e. airfare cancellation, materials, shipping, etc.). If the Motorola Solutions Worldwide Education is able to reschedule the instructor, the instructor delivery rate will be waived accordingly.
7. The effort has been made in advance to gather all relevant information to produce this proposal and is based on information available at this time. Additional information made available later may require a revision of this proposal and the price.

1.4 PRICING INFORMATION

See Schedule B- Pricing

1.5 CONTACT INFORMATION

Training Constant: Nick Trudics
Phone: 937-751-0771
Email: Nick.Trudics@motorolasolutions.com

To: Motorola Solutions, Inc.
Attention: **Melanie Leenhouts**
Phone: 616-706-1723
Email: Melanie.Leenhotorolasolutions.com

Location: Self-paced
Language: English

STATE OF MICHIGAN

SCHEDULE J- COMMANDCENTRAL AWARE PLUS

TABLE OF CONTENTS

1.	OVERVIEW.....	1
2.	COMMANDCENTRAL AWARE FEATURES.....	2
3.	COMMANDCENTRAL AWARE INTEGRATIONS.....	4
4.	VIDEO MANAGEMENT SYSTEM COMPONENT DESCRIPTIONS	5
5.	COMMANDCENTRAL AWARE TECHNICAL DISCOVERY REQUIREMENTS	7
6.	HARDWARE ENVIRONMENT REQUIREMENTS	9
7.	CONNECTIVITY AND DESIGN REQUIREMENTS	9
8.	CJIS AND COMPLIANCE	10
	STATEMENT OF WORK	10
1.1	Introduction.....	10
1.1.1	Award, Administration and Project Initiation.....	11
1.1.2	Completion and Acceptance Criteria.....	11
1.2	Project Roles and Responsibilities Overview	11
1.2.1	Motorola Project Roles and Responsibilities	11
1.2.2	Customer Project Roles and Responsibilities Overview	13
1.2.2.1	General Customer Responsibilities	15
1.2.3	Project Planning and Pre-Implementation Review.....	15
1.2.4	Project Kickoff Teleconference	16
1.3	Contract Design Review (CDR)	17
1.3.1	Contract Design Review	17
1.4	Hardware/Software.....	18
1.4.1	CloudConnect Server Staging	18
1.4.2	Workstation Installation and Configuration.....	18
1.5	Interfaces and Integration.....	19
1.5.1	ASTRO 25 Location Integration	19
1.5.2	CommandCentral Solution Geospatial Mapping Configuration.....	19
1.5.3	CommandCentral Aware Floor Plans Configuration.....	19
1.6	CommandCentral Provisioning	19
1.6.1	CommandCentral Solution.....	19
1.7	CommandCentral Online Training	20
1.8	CommandCentral Professional Consulting Services.....	20
1.9	Product Validation	21
1.9.1	Functional Demonstration.....	21
1.9.2	Interface Validation	21
1.10	Completion Milestone	22
1.11	Transition to Support And Customer SUccess.....	22
1.12	PRICING SUMMARY.....	23

SOLUTION DESCRIPTION

1. OVERVIEW

Motorola Solutions presents the following solution for Michigan's Public Safety Communications System (MPSCS).

Motorola Solutions' CommandCentral Aware solution combines disparate systems and data into an accessible interface. This single interface offers command centers a complete operating picture to support field personnel in real time. CommandCentral Aware unifies data from mapping, correlated event monitoring, analytics, and communications. This interface streamlines public safety workflows and viewpoints, enabling users to access and act on critical information.

The agency can increase the value of current investments by connecting CommandCentral Aware to other software platforms. These integrations include Computer Aided Dispatch (CAD) systems, Call Handling, Land Mobile Radio (LMR), or Video Management Systems (VMS). Users can communicate with confidence, knowing their information is hosted in the highly secure Microsoft Azure cloud.

Application Software and System Components

The CommandCentral Aware solution includes the following elements:

- CommandCentral Aware Plus with 10 Named User Licenses and 8 year subscription.
- Agency Esri Data Sets Integration.
- Accuweather Service.
- APX Next Smart Locate.
- APX NEXT ViQi Alert Integration.
- PremierOne CAD Integration for incident and/or unit location Automatic Vehicle Location (AVL).
- CommandCentral Evidence Standard 500 MB storage and 10 Named User Licenses per year.
- Avigilon Video (ACC or ACS), Video Analytics, and LPR Integration.
- One Cloud Anchor Server Hardware.
- Software Maintenance and Technical Support.
- Services as described in the Statement of Work.

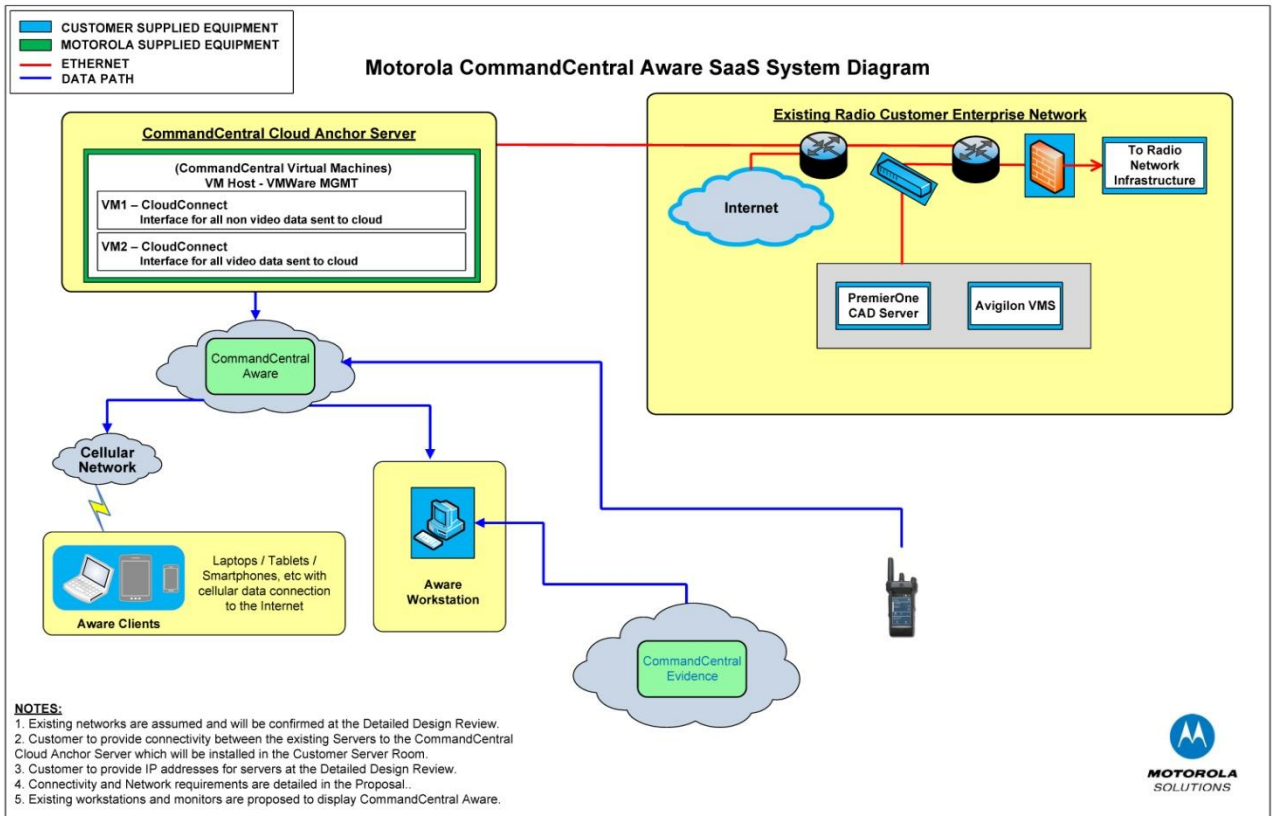


Figure 1–1: CommandCentral Aware Representative System Diagram

2. COMMANDCENTRAL AWARE FEATURES

CommandCentral Aware provides location and alert capabilities to improve public safety response, described in the sections below.

Mapping

CommandCentral Aware features a unified interface to display locations and alerts. Users can view all location-based data on the map display to enhance decision making. CommandCentral Aware Mapping features also include the following:

- **Event Monitors** – View device status and location, CAD incidents, open-source data alerts, and sensors on a map. This map can consist of Esri online, Esri server, or static map layers. This map can be modified with other data layers.
- **Data Layer Panel** – Show or hide data layers to refine the map view.
- **Event Information Display** – View details associated with each icon on the map.
- **Historical Map** – View a 90-day look back of radio locations, CAD incidents, service requests, or emergencies. An export tool extracts the recreated timeline to KML format to view in Google Earth or ESRI ArcGIS Pro. The Location Replay feature enables the historic path of a device’s location. Aware's Historical Map view enables users to interact with video assets that were available during the selected, historical time-frame. If the camera (and it's relative VMS) has the ability to play recorded footage, the recorded footage of the selected time frame can be played in Aware's Video Module directly from the Historical Map.

- Breadcrumbs – Track individual APX user radios. Tracking begins at the time the action is toggled on. Devices can provide up to the last 30 minutes of live movement.

Geographic Information System (GIS) Data Set

CommandCentral Aware integrates with hosted GIS data sets from Esri ArcGIS Server or ArcGIS online. The geospatial information contained within these data sets are core to the intelligent map display. This enhances workflow details driven by geography and the metadata contained within these data sets.

Esri's powerful geospatial engine within CommandCentral Aware is used to automatically invoke spatial queries, including nearby items and geographic boundaries. This geospatial processing enables intelligence-driven analysis in order to focus on the concentrated area of concern and orientate those responding.

Data sets help users to:

- Refine displayed data based on the geographic area defined per user. Data includes area, beat, sector, precinct, zone, or quadrant.
- Find nearby entities by predefined distance. Parameters include closest camera while in route, closest cameras to an event - CAD, gunshot detection, alert.
- Determine road blockages caused by traffic jams, flooded roadways, or other obstacles.

Rules Engine

The Command Central Aware rules engine allows users to create rule-sets to trigger actions based on event types. For example, users can highlight rows in the Event Monitor and customize sound alerts for critical incidents. These visual and audio triggers reduce the number of steps needed to support an incident.

AccuWeather

CommandCentral Aware includes integration with AccuWeather. This integration provides customized weather-driven services. Services include site-specific forecasts, severe-weather warnings, historical data, and custom analytics. AccuWeather also provides the following data:

- Location key for the desired location.
- Forecast information for a specific location.
- Current Conditions data for a specific location.
- Daily index values for a specific location. Index availability varies by location.
- Radar and satellite images.

Floor Plan Integration

CommandCentral Aware allows the ability to view building floor plans in the Map Module enabling users to see detailed building levels, switch between floors, and look for specific rooms or cameras on each floor. Clicking the map opens a floor plan widget at the bottom of the window where users can change the view between floors in a building. The Indoor Cameras Tool allows users to place cameras on the building floor it is located on, providing more granularity in locations where cameras are installed on multiple floors. Floor plan files must be in AutoCAD DXF format to be supported by CommandCentral Aware. There are twenty five (25) floors included with CommandCentral Aware. Each additional floor will incur an additional cost.

3. COMMANDCENTRAL AWARE INTEGRATIONS

CommandCentral Aware can integrate with various tools and solutions, described in the sections below.

APX NEXT SmartLocate Integration

APX NEXT SmartLocate integration provides dispatchers with accurate location data over a broadband network. This location data, combined with CommandCentral Aware functionality, enables better tracking of field personnel and improved situational awareness. SmartLocate quickly sends GPS coordinate updates and location information from the field to dispatchers, providing a more effective operating picture of any situation. This gives dispatchers a greater ability to manage incidents and allocate resources in the most efficient way possible. Broadband connectivity increases the frequency of location reporting beyond the capability of an LMR system. This improves location accuracy and enables more users to be tracked. The CommandCentral Aware tool set features many location triggers, including time, distance, push-to-talk (PTT), emergency, and accelerated cadence during emergency.

APX NEXT ViQi Hot Hit Queries

APX NEXT ViQi Hot Hit Queries are integrated to the CommandCentral Aware Map Module. When an officer or responder in the field invokes a ViQi query via APX NEXT, the hot-hit will show up on the CommandCentral Aware map. This allows the Aware user to look up additional data and situational awareness information from a ViQi query and relay that critical information to the officer in the field, dispatch, the commander or chief, and others that need to be informed.

Computer Aided Dispatch (CAD) Integration

CommandCentral Aware integrates with CAD systems to provide CAD status and event monitor capabilities. The CAD status monitor allows users to see a listing of incidents (event type, location incidents, narrative, priority, status, geographic area, and location of devices or units). The application consumes event-driven data from multiple CAD systems, allowing for real time assessment with other relevant data published to the platform, such as officer location, alarms, alerts, tips, tactical information, voice, and video.

CommandCentral Evidence Integration

CommandCentral Aware integrates with CommandCentral Evidence. This cloud-based digital evidence management application streamlines collecting, securing, and managing multimedia evidence content. This application simplifies building a secure digital evidence library by incorporating data from multiple sources into a unified storage framework. Users can upload digital evidence from a variety of sources to CommandCentral Evidence to quickly build cases.

Evidence is easy to search, correlate, and review alongside other case-related information from the RMS/CAD database. Relevant content can be marked and sorted to quickly locate critical information from a centralized touchpoint. This allows personnel to make informed decisions from a more organized and complete case evidence view, while offering an access control system to allow only authorized personnel to view sensitive information.

CommandCentral Aware users can clip videos from live or recorded video streams from CommandCentral Aware, define a start and end time for the video clip, tag the clip with an incident ID, and save a copy of the video directly to CommandCentral Evidence. This workflow is streamlined

from the CommandCentral Aware application. Native metadata from the camera source (time, date, GPS location) are automatically copied over to the video evidence within Evidence. CommandCentral Aware users can easily switch over to Evidence to perform redactions, share with external judicial partners or the public, or perform other digital evidence management tasks. Since CommandCentral Aware and Evidence both exist within the CommandCentral ecosystem, Single Sign-on is used avoiding the need for separate logon credentials.

4. VIDEO MANAGEMENT SYSTEM COMPONENT DESCRIPTIONS

As part of CommandCentral Aware, the Video View module consumes video content from a variety of Video Management Systems (live and recorded, fixed and mobile). Each VMS offers a variety of tools via an SDK. These tools can include, but are not limited to, location, user-controlled Pan Tilt Zoom (PTZ), Digital Zoom, Image Capture, Video rewind and export clip, and historic search of recorded video. These features improve productivity and increase responder safety.

The Video View module can also consume video analytics of automated license plate recognition and object detection. These capabilities refine video feeds to accurately assess detail that the eye may not see, further enhancing the users experience within CommandCentral Aware. Component configuration within CommandCentral Aware allows for specific use case definition expanding automated intelligence into the application via:

- Workflow Configuration – Associate related data from different systems to get a comprehensive view of an incident or threat. Display nearby video sources based on CAD incident, sensor alarms, and provided third-party data alerts.
- Real-Time Video Streaming – Patrol the community or view an event in seconds by accessing up to 16 cameras simultaneously from video feeds via VMS. Users can reference the video source, date, time, and location, as well as customize camera groups for quicker access to particular locations.
- Camera Field of View – Define FOV and view on the map display. Users can toggle cameras off and on that may or may not be pointed in the direction of the incident.
- Video Camera Audit Log – Capture user interactions and record them in a log.

Table -1 – Supported Video Capabilities within CommandCentral Aware

Feature	Description
Camera Import	Importing cameras and the directory tree from VMS to CommandCentral Aware.
Camera Location	Use coordinates stored in-camera custom fields at the NVR (or) pulls geo-location coordinates from the camera units. Specifically identified during installation.
PTZ	Control of pan, tilt, and zoom (PTZ) functions on capable camera units that have been imported into CommandCentral Aware.
PTZ Presets	PTZ cameras predefined pan, tilt, zoom values are applied to live feed.
PTZ Tours	PTZ cameras execute a scan of its vicinity.
Live Video	Direct feed from the camera as provisioned in the VMS system.
Recorded Video	Playback video from the archive.
Live Snapshots	Perform a screen capture of the live scene to send as an attachment via messaging service.

Recorded Snapshots	Isolate and capture a section of the recorded video to be distributed by the messaging service.
Recorded Fast Forward	Display frame recorded sample at a faster rate playing forward.
Record Fact Backward	Display frame recorded sample at a faster rate playing backward.
Digital Zoom	Magnifies a selected area for live and recorded video.
Video Export	Ability to prepare a video clipping for export to messaging or evidence collection.
Bookmark	On Live View and Recorded Playback, the bookmark automatically captures the camera information, the date, and time stamps for the video, and enables you to input the bookmark author, a name for the bookmark, and an optional description, plus an associated incident identifier. Bookmark fields can be edited later, except for the date, time, and author fields.

Avigilon Control Center (ACC) & Video Analytics

The Avigilon Control Center (ACC) uses self-learning analytics to provide effective monitoring and proactive, real-time response for security personnel. ACC combines an intuitive interface with advanced artificial intelligence (AI) search technology for a full-featured integration with CommandCentral Aware. Avigilon offers analytics embedded in Avigilon cameras up to 5K (16 MP) resolution.

This ACC integration includes the following:

- **Advanced Pattern-Based Analytics** – Avigilon advanced video pattern detection technology accurately recognizes the movements of people and vehicles while ignoring motion not relevant to a scene. The system’s self-learning ability reduces false positives and helps make alerts more meaningful.
- **Teach-by-Example Technology** – Avigilon teach-by-example object classifier technology allows users to provide feedback about the accuracy of alarm events generated by Avigilon devices. Rather than decreasing analytics sensitivity to reduce false alarms, the feedback trains devices to improve the accuracy of the analytics used to determine which alarms are real and which are false. This impacts a low false-positive alarm rate. Over time, the system learns the scene and is able to prioritize important events based on user feedback. This increases sensitivity to conditions that are of concern while reducing false alarms to keep the focus on what matters.
- **Avigilon Video Analytics Alerts Integration** – Avigilon ACC allow video analytics to send alerts to CommandCentral Aware. These analytics include object detection, motion detection, path crossed, and directional pattern changes.

The ACC rules engine enables users to selectively apply analytics-based events as alarms and rule triggers. These rules offer immediate notifications for suspicious activities to help CommandCentral Aware users monitor and respond more efficiently.

The Avigilon to CommandCentral Aware connector integrates the results of the rules engine combined with video from the Avigilon VMS. The targeted video feed is displayed in response to user interaction and pre-defined scenarios based on a customizable rule set. Users can configure specific categories of events, such as CAD incidents, LPR alarms, or other alert reporting systems integrated into CommandCentral Aware, in relation to analytics to trigger video feeds. These real-time events and forensic capabilities detect and notify scene changes, missing objects, and rules violations. In addition to the live video and analytics, the connector supplies operator’s video display tools that control pan, tilt, zoom (PTZ) cameras, and playback of recorded video.

The following is a complete list of Avigilon Control Center (ACC) video analytics features for object detection and classification for live or forensic events that enhance the common operating picture and situational awareness capabilities of CommandCentral Aware.

Table 1-2 – Avigilon Control Center Video Analytics

Avigilon Analytics Rules for ACC	Analytics Rules Description (Objects are Classified as Person or Vehicle)
Objects in Area	The event is triggered when the selected object type moves into a specified region of interest.
Object Loitering	The event is triggered when the selected object type stays within a specified region of interest for an extended amount of time which is configured.
Objects Crossing Beam	The event is triggered when an Object or a specified number of Objects have crossed the directional beam that has been configured over the camera's field of view. The beam can be unidirectional or bidirectional.
Object Appears of Enters Area	The event is triggered by each object that enters the specified region of interest.
Object Not Present in Area	The event is triggered when no objects are present in the specified region of interest.
Objects Enter Area	The event is triggered when the specified number of objects have entered the specified region of interest.
Objects Leave Area	The event is triggered when the specified number of objects has left a specified region of interest region of interest.
Object Stops In Area	The event is triggered when an object in a specified region of interest stops moving for the specified threshold time.
Direction violated	The event is triggered when an object moves in the prohibited direction of travel.
Camera tampering	The event is triggered due to sudden scene changes.
License Plate Recognition Analytics	New license plate recognition analytics engine with highly-accurate license plate capture, identification, and search for fast event response. Use watch lists to create alerts and actions when a license plate match is detected.

5. COMMANDCENTRAL AWARE TECHNICAL DISCOVERY REQUIREMENTS

In order to prevent delay in the implementation, Customer must provide the information required in the table below at the time of Project Kickoff for each interface/integrated system.

Table 1-3: Aware Technical Discovery Requirements

	Customer Provided	Motorola Confirmed
Additional Information for Virtual Machine (VM) Access		
Remote access to Cloud Anchor Server		
Data Interface VM requirements		
Video Interface VM requirements		

Interfaces (Required for each Interface)		
Manufacturer and Current Software Version		
Confirm API/SDK Availability		
Provide IP Addresses		
Provide Data format		
Provide Data Frequency (Peak & average events & content)		
Provide Operational aspects (data latency, key fields/information, # inputs)		
Data path factors (bandwidth, NAT, latency, jitter)		
Additional VMS Interface Requirements		
<ul style="list-style-type: none"> Number of Cameras connected to each VMS 		
<ul style="list-style-type: none"> VMS Archive and Archiver to Aware Client 		
<ul style="list-style-type: none"> Provide GPS Coordinates for each camera 		
Integration		
Customer IP Network layout (Traffic segmentation, NAT required?)		
Active Directory and Email policies		
Customer Third-Party IP Network Connections (Schools, Fire, Traffic)		
Remote Access Policy/Procedures		
Who owns/maintains each Customer network/firewalls?		
Additional Information Required for Integration with CAD & ALPR Systems		
Data delivery latency rate		
Data interface type		
<ul style="list-style-type: none"> Fileshare/Dump 		
<ul style="list-style-type: none"> Webservices 		
<ul style="list-style-type: none"> SOAP/REST 		
<ul style="list-style-type: none"> SQL Extraction 		
Database IP Address, Login Credentials, DB Version		
Data volume (calls per service, peak event rates)		
Data Fields		
<ul style="list-style-type: none"> CAD event Geolocation data availability 		
<ul style="list-style-type: none"> AVL/ARL data available? 		
<ul style="list-style-type: none"> Event Types 		

• Icons		
• Others(?)		
Additional Information Required for Integration with Streaming Servers		
Mobile data terminal types:		
• Manufacturer		
• OS version		
• Wireless Access		
• VPN Connectivity to Core?		
• Validate Data Ingestion (may require system expansion**)		

6. HARDWARE ENVIRONMENT REQUIREMENTS

Cloud Anchor Server

- One rack unit per Cloud Anchor server.
- Two circuits to distribute power to the server rack (dual power supplies).
- UPS (Uninterruptible Power Supply) at the site where the Cloud Anchor server and CommandCentral Aware workstations will be installed.
- Access to the Internet

Customer-Provided Aware Workstation (minimum requirements)

- **Processor** - Intel Xeon 6136 @3.0 GHz (12 cores).
- **Memory** - 32 GB.
- **Drive** - One NVMe 512G SSD.
- **NIC** - 1 Gb port NIC.
- **OS** - Windows 7 Professional or Windows 10 Professional.
- **Graphics Card** - NVIDIA Quadro P2000.

Customer-Provided Workstation Monitors (minimum requirements)

- 27-inch Narrow Bezel IPS Display, 2560X1440.

7. CONNECTIVITY AND DESIGN REQUIREMENTS

Motorola Solutions will work with the Customer IT personnel to verify that connectivity meets requirements. The Customer will provide the network components.

Network Physical Requirements

- Three static IP addresses, corresponding subnet masks/default gateway, and available NTP and DNS IP to the Cloud Anchor Server.
- One network port for each VMS server.
- One network port for each VMS analytics appliance.

Network Bandwidth Requirements

- Provide network ports that are 1GB capable and network routable.

- Minimum bandwidth needed between the Cloud Anchor Server and the CommandCentral Aware platform is 1.1 Mbps.

Low latency is critical for real-time operations. The speed with which data appears on the CommandCentral Aware display depends in large part on how quickly the information is presented to the CommandCentral Aware interface. Major contributors to the latency are network delays and the delay time from occurrence of an event to when that event information is presented to Aware from the source application (CAD, AVL, ALPR). Although CommandCentral Aware strives to provide near-real-time performance, Motorola Solutions provides no guarantees as to the speed with which an event (or video stream) appears in the application once the event is triggered.

CommandCentral Aware Design Limitations

- A maximum of 3000 Icons viewed on the CommandCentral Aware client at one time, per instance.
- A maximum of 100 updates per second on the CommandCentral Aware client.
- A maximum 5000 radios per server.

Broadband Locationing Requirements

Broadband devices require a data subscription. The broadband subscription is not included in the price of the CommandCentral Aware offer. Android and iOS devices will require Motorola Solutions client software to be installed on each device.

Broadband Infrastructure Requirements

Broadband networks should provide connectivity over 4G LTE, or fourth-generation mobile data technology Long-term Evolution, as defined by the International Telecommunication Union's Radio Sector (ITU-R) and/or Wi-Fi defined as IEEE Standard 802.11 (preferably 802.11ac or 802.11n).

8. CJIS AND COMPLIANCE

At Motorola Solutions, we believe compliance is a team effort. As our customers' partner in compliance, we employ privacy and security protocols that enable our customers to comply with the most stringent legal and regulatory requirements. In addition, we build on a strong foundation with an Azure architecture designed and managed to meet a broad set of international compliance standards, as well as region-specific and industry-specific standards.

Motorola Solutions employs rigorous third-party audits to verify its adherence to security controls and standards. To demonstrate Motorola Solutions safeguarding of customer data, comprehensive third-party audits of primary Software Enterprise development and support operations have been completed and those operations have achieved ISO/IEC 27001:2013 (information security management systems) certification and AICPA SOC2 Type 2 reports will be available in early 2021. ISO/IEC 27017:2015 (information security controls for cloud services), ISO/IEC 27018:2019 (protection of personal information in public clouds) and ISO/IEC 27701:2019 (privacy information management) will be available in mid-2021. Supplemental SOC2 Type 2 reports and ISO/IEC 27001:2013 certifications for the development and support operations at satellite locations will be complete by the end of 2021.

Motorola Solutions understands our customers' critical need to safeguard the lifecycle of Criminal Justice Information. To support that need, Motorola Solutions designs its products and services to support compliance with the FBI's Criminal Justice Information Services (CJIS) Security Policy and we commit to the terms of the CJIS Security Addendum. With a dedicated team of CJIS compliance professionals, we assist our customers through administering and coordinating CJIS-compliant personnel credentialing, providing documentation assistance in connection with CJIS audits, and

advising on how to configure and implement our solutions in a manner consistent with the CJIS Security Policy.

STATEMENT OF WORK

1.1 INTRODUCTION

In accordance with the terms and conditions of the Agreement, this Statement of Work (“SOW”) defines the principal activities and responsibilities of all parties for the delivery of the Motorola Solutions (“Motorola”) system as presented in this offer to Michigan Department of Information Tech DNB FIN SVC (hereinafter referred to as “Customer”). When assigning responsibilities, the phrase “Motorola” includes our subcontractors and third-party partners.

Deviations and changes to this SOW are subject to mutual agreement between Motorola and the Customer and will be addressed in accordance with the change provisions of the Agreement.

Unless specifically stated, Motorola work is performed remotely. Customer will provide Motorola resources with unrestricted direct network access to enable Motorola to fulfill its delivery obligations.

Motorola and the Customer will work to complete their respective responsibilities in accordance with the mutually agreed upon governing Project Schedule. Any changes to the governing Project Schedule will be mutually agreed upon via the change provision of the Agreement.

The number and type of software or subscription licenses, products, or services provided by Motorola or its subcontractors are specifically listed in the Agreement and any reference within this document as well as subcontractors’ SOWs (if applicable) does not imply or convey a software or subscription license or service that are not explicitly listed in the Agreement.

1.1.1 Award, Administration and Project Initiation

Project Initiation and Planning will begin following execution of the Agreement between Motorola and the Customer.

Following the conclusion of the Project Planning Session, the Motorola Project Manager will conduct twice monthly one-hour remote status meetings with the Customer Project Manager for the purpose of baselining progress of current activities and the planning of future activities. Following the conclusion of the Contract Design Review, the Motorola Project Manager will prepare and submit monthly status reports to the Customer Project Manager. Monthly Status Reports provide a summary of the activities completed in the month, those activities planned for the following month, project progress against the project schedule, items of concern requiring attention as well as potential project risks and agreed upon mitigation actions.

1.1.2 Completion and Acceptance Criteria

Motorola Integration Services are considered complete upon Motorola performing the last task listed in a series of responsibilities or as specifically stated in Completion Criteria. Customer task completion will occur per the project schedule enabling Motorola to complete its tasks without delay.

Customer will provide Motorola written notification that it does not accept the completion of Motorola responsibilities or rejects a Motorola service deliverable within five (5) business days of completion or receipt of a deliverable.

The Service Completion will be acknowledged in accordance with the terms of Master Customer Agreement and the Service Completion Date will be memorialized by Motorola and Customer. Software System Completion will be in accordance with the terms of the Software Products Addendum unless otherwise stated in this Statement of Work.

1.2 PROJECT ROLES AND RESPONSIBILITIES OVERVIEW

1.2.1 Motorola Project Roles and Responsibilities

A Motorola team, made up of specialized personnel, will be appointed to the project under the direction of the Motorola Project Manager. Team members will be multi-disciplinary and may fill more than one role. Team members will be engaged in different phases of the project as necessary.

In order to maximize efficiencies Motorola's project team will provide services remotely via teleconference, web-conference or other remote method in filling its commitments as outlined in this Statement of Work. Motorola project team resources will be on site at the Customer location when fulfilling commitments that are crucial to project success as noted in this Statement of Work.

The personnel role descriptions noted below provide an overview of typical project team members. There may be other personnel engaged in the project under the direction of the Project Manager. The following provided descriptions of the primary roles engaged in the delivery of the project. One or many resources of the same type may be engaged as needed throughout the project.

Motorola's project management approach has been developed and refined based on lessons learned in the execution of hundreds of system implementations. Using experienced and dedicated people, industry-leading processes, and integrated software tools for effective project execution and control, we have developed and refined practices that support the design, production, and testing required to deliver a high-quality, feature-rich system.

Project Manager

A Motorola Project Manager will be assigned as the principal business representative and point of contact for the organization. The Project Manager's responsibilities include:

1. Manage the Motorola responsibilities related to the delivery of the project.
2. Maintain the project schedule and manage the assigned Motorola personnel and applicable subcontractors/supplier resources.
3. Manage the Change Order process per the Agreement.
4. Maintain project communications with the Customer.
5. Identify and manage project risks.
6. Collaborative coordination of Customer resources to minimize and avoid project delays.
7. Measure, evaluate, and report the project status against the Project Schedule.
8. Conduct remote status meetings on a mutually agreed basis to discuss project status.

9. Prepare and submit a monthly status report that identifies the activities of the previous month, as well as activities planned for the current month, including an updated Project Schedule and action item log.
10. Provide timely responses to issues related to project progress.

Solutions Architect

The Solutions Architect is responsible for the delivery of the technical and equipment elements of the solution. They confirm the delivered technical elements meet contracted requirements. They are engaged throughout the duration of the delivery.

Customer Success Advocate

A Customer Success Advocate will be assigned to the Customer post Go Live event. By being the Customer's trusted advisor, the Customer Success Advocate's responsibilities include:

- Assist the Customer with maximizing the use of their Motorola software and service investment.
- Actively manage, escalate, and log issues with Support, Product Management, and Sales.
- Provide ongoing customer communication about progress, timelines, and next steps.

Customer Support Services Team

The Customer Support Services team will provide ongoing support following commencement of beneficial use of the Customer's System(s) as defined in Customer Support Plan.

1.2.2 Customer Project Roles and Responsibilities Overview

The success of the project is dependent on early assignment of key Customer resources. It is critical these resources are empowered to make provisioning decisions based on the Customer's operational and administration needs. The Customer project team should be engaged from project initiation through beneficial use of the system. The continued involvement in the project and use of the system will convey the required knowledge to maintain the system post completion of the project. In some cases, one person may fill multiple project roles. The project team must be committed to participate in activities for a successful implementation.

Project Manager

The Project Manager will act as the primary Customer point of contact for the duration of the project. In the event the project involves multiple agencies, Motorola will work exclusively with a single Customer assigned Project Manager (the primary Project Manager). This includes the management of any third party vendors that are Customer Subcontractors. The Project Manager's responsibilities include:

1. Communicate and coordinate with other project participants.
2. Manage the Customer project team including timely facilitation of efforts, tasks, and activities.
3. Maintain project communications with the Motorola Project Manager.
4. Identify the efforts required of Customer staff to meet the task requirements and milestones in this SOW and Project Schedule.
5. Consolidate all project-related questions and queries from Customer staff to present to the Motorola Project Manager.

6. Review the Project Schedule with the Motorola Project Manager and finalize the detailed tasks, task dates, and responsibilities.
7. Measure and evaluate progress against the Project Schedule.
8. Monitor the project to ensure resources are available as scheduled.
9. Attend status meetings.
10. Provide timely responses to issues related to project progress.
11. Liaise and coordinate with other agencies, Customer vendors, contractors, and common carriers.
12. Review and administer change control procedures, hardware and software certification, and all related project tasks required to maintain the Project Schedule.
13. Ensure Customer vendors' adherence to overall Project Schedule and Project Plan.
14. Assign one or more personnel who will work with Motorola staff as needed for the duration of the project, including at least one representative(s) from the IT department.
15. Identify the resource with authority to formally acknowledge and approve Change Orders, approval letter(s), and milestone recognition certificates as well as approve and release payments in a timely manner.
16. Provide building access to Motorola personnel to all Customer facilities where system equipment is to be installed during the project. Temporary identification cards are to be issued to Motorola personnel if required for access to facilities.
17. Ensure remote network connectivity and access to Motorola resources.
18. As applicable to this project, assume responsibility for all fees for licenses and inspections and for any delays associated with inspections due to required permits.
19. Provide reasonable care to prevent equipment exposure to contaminants that cause damage to the equipment or interruption of service.
20. Ensure a safe work environment for Motorola personnel.
21. Provide signatures of Motorola-provided milestone certifications and Change Orders within five (5) business days of receipt.

Transformation Lead

The Transformation Lead, who may or may not be your Project Manager, must be able to holistically represent your organization and be able to work cross functionally between Motorola, your organization, and all stakeholders involved in the delivery of your new system. The Transformation Lead must be empowered to acknowledge the resource and time commitments required of your organization and authorize Motorola to proceed with scheduling the Project Kickoff event.

System Administrator

The System Administrator manages the technical efforts and ongoing tasks and activities of their system as defined in the Customer Support Plan (CSP).

IT Personnel

IT personnel provide required information related to LAN, WAN, wireless networks, server, and client infrastructure. They must also be familiar with connectivity to internal, external, and third-party systems to which the Motorola system will interface.

Additional Resources

Additional resources, such as trainers and database administrators may also be required.

User Agency Stakeholders

User Agency Stakeholders, if the system is deployed in a multi-agency environment, are those resources representing agencies outside of the Customer's agency. These resources will provide provisioning inputs to the SMEs if operations for these agencies differ from that of the Customer agency.

1.2.2.1 General Customer Responsibilities

In addition to the Customer Responsibilities stated elsewhere in this SOW, the Customer is responsible for:

1. All Customer-provided equipment including hardware and third-party software necessary for delivery of the System not specifically listed as a Motorola deliverable. This will include end user workstations, network equipment, telephone, or TDD equipment and the like.
2. Configuration, maintenance, testing, and supporting the third-party systems the Customer operates which will be interfaced to as part of this project. The Customer is responsible for providing Application Programming Interface (API) documentation to those systems that document the integration process for the level of interface integration defined by Motorola.
3. Initiate, coordinate, and facilitate communication between Motorola and Customer's third-party vendors as required to enable Motorola to perform its duties.
4. Active participation of Customer Subject Matter Experts (SME's) in project delivery meetings and working sessions during the course of the project. Customer SME's will possess requisite knowledge of Customer operations and legacy system(s) and possess skills and abilities to operate and manage the system.
5. The provisioning of Customer GIS data as requested by Motorola. This information must be provided in a timely manner in accordance with the Project Schedule.
6. Electronic versions of any documentation associated with the business processes identified.
7. Providing a facility with the required computer and audio-visual equipment for training and work sessions as defined in the Training Plan.
8. Ability to participate in remote project meeting sessions using Google Meet.

1.2.3 Project Planning and Pre-Implementation Review

A clear understanding of the needs and expectations of both Motorola and the Customer are critical to the successful implementation and on-going operation of CommandCentral. In order to establish initial expectations for system deployment and to raise immediate visibility to ongoing operation and maintenance requirements, we will work with you to help you understand the impact of introducing a new solution and your preparedness for the implementation and support of the CommandCentral system.

Shortly after contract signing, Motorola will conduct a one-on-one teleconference with your designated resource to review the task requirements of each phase of the project and help to identify areas of potential risk due to lack of resource availability, experience or skill.

The teleconference discussion will focus on the scope of implementation requirements, resource commitment requirements, cross-functional team involvement, a review of the required technical resource aptitudes and a validation of existing skills, and resource readiness in preparation for the Project Kickoff meeting.

Motorola Responsibilities

1. Make initial contact with the Customer Project Manager and schedule the Pre-Implementation Review teleconference.
2. Discuss the overall project deployment methodologies, inter-agency/inter-department decision considerations (as applicable), and third party engagement/considerations (as applicable).
3. Discuss Customer involvement in system provisioning and data gathering to understand scope and time commitment required.
4. Discuss the online Learning Management System (LMS) training approach.
5. Obtain mutual agreement of the Project Kickoff meeting agenda and objectives.
6. Discuss the CommandCentral Solution Discovery Requirements checklist and verify Customer has a copy of the checklist.
7. Coordinate enabling designated Customer administrator with access to the LMS and CommandCentral Admin Console.

Customer Responsibilities

1. Provide Motorola with the names and contact information for the designated LMS and application administrators.
2. Collaborate with the Motorola PM and set the Project Kickoff meeting date.

1.2.4 Project Kickoff Teleconference

The purpose of the project kickoff is to introduce project participants and review the overall scope of the project.

Motorola Responsibilities

1. Conduct a project kickoff teleconference.
2. Validate key project team participants attend the meeting.
3. Introduce all project participants.
4. Review the roles of the project participants to identify communication flows and decision-making authority between project participants.
5. Review the overall project scope and objectives.
6. Review the resource and scheduling requirements.
7. Review the teams' interactions (meetings, reports, milestone acceptance) and Customer participation.
8. Verify Customer Administrator(s) have access to the LMS and CommandCentral Admin Console.

Customer Responsibilities

1. Validate key project team participants attend the meeting.

2. Introduce all project participants.
3. Review the roles of the project participants to identify communication flows and decision-making authority between project participants.
4. Provide VPN access to Motorola staff to facilitate delivery of services described in this Statement of Work.
5. Validate any necessary non-disclosure agreements, approvals, and other related issues are complete in time so as not to introduce delay in the project schedule. Data exchange development must adhere to third-party licensing agreements.
6. Provide all paperwork and/or forms (i.e. fingerprints, background checks, card keys and any other security requirement) required of Motorola resources to obtain access to each of the sites identified for this project.
7. Provide the contact information for the license administrator for the project. I.e. IT Manager, CAD Manager, and any other key contact information as part of this project.
8. Validate access to the LMS and CommandCentral Admin Console.
9. Provide the information required in the CommandCentral Solution Discovery Requirements checklist.

1.3 CONTRACT DESIGN REVIEW (CDR)

1.3.1 Contract Design Review

The objective is to review the contracted applications, project schedule, bill of materials, functional demonstration approach and contractual obligations of each party. The CDR commences upon conclusion of the Project Kickoff session.

Any changes to the contracted scope can be initiated via the change provision of the Agreement.

Motorola Responsibilities

1. Review the Ordering Documents: System Description, Statement of Work and Project Schedule.
2. Review the technical, environmental and network requirements of the system.
3. Review the initial Project Schedule and incorporate Customer feedback resulting in the implementation project schedule. The project schedule will be maintained by Motorola and updated through mutual collaboration. Schedule updates that impact milestones will be addressed via the change provision of the Agreement.
4. Review and order contacted hardware.
5. Review the functional demonstration process for CommandCentral Solution and interfaces.
6. Request shipping address and receiver name.
7. Provide completed paperwork, provided to Motorola during project kickoff that enables Motorola resources to obtain site access.
8. Review the information in the Customer provided CommandCentral Solution Discovery Requirements checklist.
9. Grant Customer Administrator with access to CommandCentral Admin Console.

10. Grant Customer LMS Administrator with access to the LMS.
11. Generate a CDR Summary report documenting the discussions, outcomes and any required change orders.

Customer Responsibilities

1. Project Manager and key Customer assigned designees attend the meeting.
2. Provide network environment information as requested.
3. Providing shipping address and receiver name.
4. Provide locations and access to the existing data and video equipment that will be part of the CommandCentral system per the Agreement.

Completion Criteria

The CDR is complete upon Customer receipt of the CDR Summary report.

1.4 HARDWARE/SOFTWARE

Hardware and software activities account for the procurement, staging and configuration of server hardware.

1.4.1 CloudConnect Server Staging

The objective of this activity is to install the software components on the server procured by Motorola at our staging facility. The server will be tested and verified to be operational in a staged environment. Once validated, the server will be packaged and shipped to the Customer’s location for installation.

Motorola Responsibilities

1. Order contracted server related components for delivery to the staging facility.
2. Install and configure system software.
3. Ship staged system to the Customer’s installation site.

Customer Responsibilities

1. Receive the staged server and securely store it until Motorola installation.
2. Provide power and assign network IP addresses. Provide backup power, as necessary.
3. Provide network connectivity between the various networks.
4. Provide acknowledgement of receipt of delivered equipment.

Motorola Deliverables

Title/Description
Equipment Inventory
Staged System Delivery

1.4.2 Workstation Installation and Configuration

The objective of this activity is to configure and install Customer provided workstation and monitors.

Motorola Responsibilities

1. Verify remote access capability after Customer completes physical installation.
2. Configure workstations and monitors for CommandCentral Aware.

Customer Responsibilities

1. Perform physical installation of the CommandCentral Aware workstations. Connect to power and network. Assign IP addresses for the network.
2. Provide remote access to the CommandCentral Aware workstations.

Completion Criteria

CommandCentral Solution workstation configuration is complete.

1.5 INTERFACES AND INTEGRATION

The installation, configuration and demonstration of interfaces may be an iterative series of activities depending upon access to third-party systems. Interfaces will be installed and configured in accordance with the project schedule. Integrations of functionality between Motorola developed products will be completed through software installation and provisioning activities in accordance with the Project Schedule dates. Integration activities that have specific requirements will be completed as outlined in this SOW.

1.5.1 CommandCentral Solution Geospatial Mapping Configuration

Motorola Responsibilities

1. Installation and configuration of the connection to the Customer mapping system, (i.e. ESRI online, ESRI server, or static map layers).
2. Add camera locations to ESRI system map and configure hot links within CommandCentral Solution system.
3. Test mapping layers and links to validate CommandCentral Solution is accessing and utilizing Customer published GIS data.

Customer Responsibilities

1. Provide access to ESRI/GIS system and/or GIS personnel.
2. Provide published GIS map layers.
3. Work with Motorola staff to publish specific maps beneficial to the Customer analysts.

Completion Criteria

CommandCentral Solution Geospatial Mapping configuration is complete.

1.5.2 CommandCentral Aware Floor Plans Configuration

Motorola Responsibilities

1. Import the floor plans into CommandCentral Solution.
2. Add camera locations to floor plan(s) and configure hot links within CommandCentral Solution system.
3. Test floor plan layers and validate CommandCentral Solution is accessing and utilizing floor plans in the correct location and orientation.

Customer Responsibilities

1. Provide floor plan files in the acceptable formats.

Completion Criteria

CommandCentral Solution Floor Plans configuration is complete.

1.6 COMMANDCENTRAL PROVISIONING

1.6.1 CommandCentral Solution

Motorola will discuss industry best practices, current operations environment and subsystem integration in order to determine the optimal configuration for CommandCentral Solution.

Motorola Responsibilities

1. Using the CommandCentral Admin Console, provision users, groups, rules and based off Customer Active Directory data.

Customer Responsibilities

1. Supply the access and credentials to Customer's Active Directory for the purpose of Motorola conducting CommandCentral Solution provisioning.
2. Respond to Motorola inquiries regarding users/groups/agency mapping to CommandCentral Solution functionality.

Completion Criteria

CommandCentral Solution provisioning is complete upon Motorola completing provisioning activities.

1.7 COMMANDCENTRAL ONLINE TRAINING

CommandCentral training is made available to via Motorola Solutions Software Enterprise Learning Management System (LMS). This subscription service provides you with continual access to our library of online learning content and allows your users the benefit of learning at times convenient to them. Content is added and updated on a regular basis to keep information current. All Motorola Solutions tasks are completed remotely and enable the Customer to engage in training when convenient to the user.

LMS Administrators are able to add/modify users, run reports, and add/modify groups within the panorama.

Motorola Solutions Responsibilities

- Initial setup of Panorama and addition of administrators.
- Provide instruction to the Customer LMS Administrators on:
 - Adding and maintaining users.
 - Adding and maintaining Groups.
 - Assign courses and Learning Paths.
 - Running reports.

Customer Responsibilities

- Go to <https://learningservices.Motorola Solutions.com> and request access if you do not already have it.
- Complete LMS Administrator training.
- Advise users of the availability of the LMS.
- Add/modify users, run reports and add/modify groups.

Completion Criteria

Work is considered complete upon conclusion of Motorola Solutions provided LMS Administrator instruction.

Panorama – A panorama is an individual instance of the Learning Management System that provides autonomy to the agency utilizing.

Groups – A more granular segmentation of the LMS that are generally used to separate learners of like function (i.e. dispatchers, call takers, patrol, firefighter). These may also be referred to as clients within the LMS.

Learning Path – A collection of courses that follow a logical order, may or may not enforce linear progress.

1.8 COMMANDCENTRAL PROFESSIONAL CONSULTING SERVICES

Professional Consulting Services provide the Customer an opportunity to utilize Motorola subject matter experts as needed to address operational concerns: impromptu training, process re-engineering or one on one personalized support.

Motorola Responsibilities

1. Conduct a discovery teleconference with Customer's PM to understand the Customer needs prior to scheduling on-site service.
2. Provide Customer with a summary of the needs discussed during the teleconference that serve as the focus for the on-site service delivery.
3. Upon agreement of the focus of on-site service, schedule a mutually agreeable date for delivery of on-site service.
4. Provide six days total spread across two trips of on-site service Monday through Friday, 8:00 am to 5:00 pm Customer time.

5. Provide Customer with a summary report of the activities completed as part of on-site service delivery.

Customer Responsibilities

1. Participate in the discovery teleconference and agree to objectives.
2. Schedule a mutually agreeable date for delivery of on-site service.
3. Coordinate availability of people or resources required for Motorola to fulfill the focus of on-site service.

Completion Criteria

Work is considered complete upon Motorola providing Customer with the summary report.

1.9 PRODUCT VALIDATION

The system is exercised throughout the delivery of the project by both Motorola and the Customer via provisioning and training activities. To solidify Customer confidence in the system and prepare for user operation, Motorola will perform prescribed system validations in accordance with a Product Validation Plan.

1.9.1 Functional Demonstration

The objective of functional demonstration is to validate Customer access to the CommandCentral features and functions and system integration via configured interfaces (as applicable).

Motorola Responsibilities

1. Update functional demonstration script.
2. Provide script to Customer for review and acknowledgement.
3. Conduct functional demonstration.
4. Correct any configuration issues impacting access to cloud based features; i.e. map display, location updates, video display and/or interface and integrations.
5. Create a summary report documenting the activities of the functional demonstration and any corrective actions taken by Customer or Motorola during the demonstration.
6. Provide Customer instruction on using the Customer Feedback Tool for feature/enhancement requests.

Customer Responsibilities

1. Review and agree to the scope of the demonstration script.
2. Witness the functional demonstration and acknowledge its completion.
3. Resolve any provisioning impacting the functional demonstration.
4. Provide Motorola with any requests for feature enhancements.

Completion Criteria

Conclusion of the functional demonstration.

1.9.2 Interface Validation

The objective of Interface Validation is to verify that the installed interfaces perform in accordance with what is presented in the System Description.

Motorola is not responsible for issues arising from lack of engagement of third-party and/or Customer resources to perform work required to enable/provision and/or configure an interface to a third-party system, or troubleshooting any issues on the Customer's third-party systems.

Interfaces that cannot be tested due to connectivity issues to external systems, or the unavailability of Customer's third-party system will be demonstrated to show that Motorola's portion of an interface is enabled to send and/or receive data that supports the interface experience. In such cases, Motorola demonstrating the elements within Motorola's control will constitute a successful demonstration and completion of the demonstration task.

Motorola Responsibilities

1. Conduct Interface Validation demonstration.
2. Develop remediation plan for anomalies that do not align with Motorola's stated System Description.

Customer Responsibilities

1. Provide access to a resource with access to the interfacing system to validate functionality.
2. Witness the execution of the demonstration and acknowledge successful completion.
3. Participate in the documentation of anomalies and work with Motorola to develop remediation action(s).

Motorola Deliverable

Title/Description
Remediation Plan/Schedule for documented anomalies, as required

1.10 COMPLETION MILESTONE

Following the conclusion of delivery of the functional demonstration the project is considered complete and the Software System completion milestone will be recognized.

1.11 TRANSITION TO SUPPORT AND CUSTOMER SUCCESS

Following the completion of the activation of CommandCentral components, implementation activities are complete. The transition to the Motorola Solutions' support organization completes the implementation activities.

Customer Success is the main point of contact as you integrate this solution into your agency's business processes. Our team will work with you to ensure Video-as-a-Service has met your expectations and that the solution satisfies your goals and objectives. Contact Customer Success at CommandCentralCS@motorolasolutions.com.

Our Customer Support team will be the point of contact for technical support concerns you might have and can be reached either by phone at 1-800-MSI-HELP (option x4, x4, x3) or by emailing support-commandcentral@motorolasolutions.com.

Motorola Solutions Responsibilities

- Provide the Customer with Motorola Solutions support engagement process and contact information.
- Gather contact information for the Customer users authorized to engage Motorola Solutions support.

Customer Responsibilities

- Provide Motorola Solutions with specific contact information for those users authorized to engage Motorola Solutions' support.
- Engage the Motorola Solutions support organization as needed.

Completion Criteria

Conclusion of the handover to support and the implementation project is complete.

1.12 PRICING

An initial, onetime activation fee will be charged at the inception of this work in the amount of \$153,880.00. Annual pricing is as listed in Schedule B- Pricing.



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number 2
 to
 Contract Number 190000001544

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago, IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Kate Jannereth	DTMB
		517-881-1031	
	jannerethk@Michigan.gov		
	Contract Administrator	Valerie Hiltz	DTMB
(517) 249-0459			
hiltzv@michigan.gov			

CONTRACT SUMMARY

MPSCS CONTINUED SYSTEM UPDATES, EQUIPMENT, MAINTENANCE AND UPGRADES, AND ANCILLARY SYSTEMS PRODUCTS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
October 1, 2019	December 31, 2029	0 - 0 Year	December 31, 2029
PAYMENT TERMS		DELIVERY TIMEFRAME	
NET 45		As per Delivery Order	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

N/A

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		December 31, 2029
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$99,900,000.00	\$0.00	\$99,900,000.00		

DESCRIPTION

Effective July 1, 2021 this contract is adding scope to Schedule A via Attachment 10- Critical Connect Subscription Service, adding Schedule H- Subscription Services Schedule, and updating Schedule B, all as attached.

All other terms, conditions, specifications and pricing remain the same. Per Contractor and Agency agreement and DTMB Central Procurement Services approval.



SCHEDULE A, ATTACHMENT 10

STATEMENT OF WORK FOR CRITICAL CONNECT SUBSCRIPTION SERVICES

TABLE OF CONTENTS

Section 1

Applicability	1-1
---------------------	-----

Section 2

System Description	2-1
2.1 Executive Summary	2-1
2.2 Critical Connect Solution Description	2-2
2.2.1 Sensitive Data Encryption	2-4
2.2.2 Restricted Traffic	2-4
2.2.3 Secure Access	2-4
2.2.4 P25 ISSI (LMR-LMR Interoperability).....	2-4
2.2.5 Site Link Interface (LMR-BB).....	2-4
2.2.6 ASTRO Connectivity Service configured with Critical Connect Capacity.....	2-6
2.2.7 Critical Connect Portal	2-7
2.3 Additional Critical Connect Interfaces.....	2-8
2.3.1 Radio-over-IP (ROIP) Link	2-8
2.3.2 MOTOTRBO Link	2-9
2.3.3 Data Interface	2-9
2.4 WAVE PTT Solution Overview.....	2-11
2.4.1 WAVE Administration Portal.....	2-14
2.5 Infrastructure Updates	2-15
2.6 Responsibility Matrix	2-15

Section 3

Critical Connect - Statement of Work For Installation and Onboarding.....	3-1
3.1 Contract.....	3-1
3.1.1 Contract Award (Milestone).....	3-1
3.1.2 Contract Administration	3-1
3.2 Contract Document Review	3-2
3.2.1 Review Contract Document	3-2
3.3 Order Processing	3-2



- 3.3.1 Process Equipment List..... 3-2
- 3.3.2 Install Enablement Server (WRG) Server Equipment 3-3
- 3.4 Functional Acceptance Testing 3-4
 - 3.4.1 Perform Functional Testing 3-4
 - 3.4.2 System Acceptance Test Procedures (Milestone) 3-5
- 3.5 Project Schedule..... 3-5

Section 4

- Critical Connect - Statement of Work For Request Fulfillment 4-1
 - 4.1 Agreement..... 4-1
 - 4.2 Request Fulfillment by Service Desk 4-1
 - 4.2.1 Service Desk..... 4-1
 - 4.2.2 Fulfillment Service Process Descriptions 4-2
 - 4.2.3 Roles and Responsibilities 4-2
 - 4.3 Critical Connect Technical Support 4-3
 - 4.3.1 Fulfillment Service Description 4-3
 - 4.3.2 Roles and Responsibilities 4-3
 - 4.4 Infrastructure Hardware Repair..... 4-4
 - 4.5 Critical Connect On-Site Support 4-4
 - 4.5.1 On-Site Support Description..... 4-4
 - 4.5.2 Scope 4-5
 - 4.5.3 Roles and Responsibilities 4-5

Section 5

- ASTRO 25 Connectivity Services 5-1
 - 5.1 Overview 5-1
 - 5.2 Prerequisites..... 5-1
 - 5.3 Product and Installation 5-2
 - 5.3.1 Scope 5-2
 - 5.3.2 Motorola Solutions Responsibilities 5-2
 - 5.3.3 MPSCS Responsibilities 5-2
 - 5.3.4 Availability Commitment..... 5-4
 - 5.3.5 Service Priority Levels 5-5
 - 5.3.6 ASTRO 25 Connectivity Service Sites and Equipment 5-6
 - 5.4 Availability Reports..... 5-6
 - 5.4.1 Description of Service..... 5-6
 - 5.4.2 Scope 5-7
 - 5.4.3 Inclusions..... 5-7
 - 5.4.4 Motorola Solutions Responsibilities 5-7
 - 5.4.5 Limitations and Exclusions..... 5-7



- 5.4.6 MPSCS Responsibilities 5-7
- 5.5 Backhaul Event Monitoring 5-8
 - 5.5.1 Description of Service 5-8
 - 5.5.2 Scope 5-8
 - 5.5.3 Inclusions 5-8
 - 5.5.4 Motorola Solutions Responsibilities 5-8
 - 5.5.5 Limitations and Exclusions 5-9
 - 5.5.6 MPSCS Responsibilities 5-9
- 5.6 Remote Technical Support 5-10
 - 5.6.1 Description of Service 5-10
 - 5.6.2 Scope 5-10
 - 5.6.3 Motorola Solutions Responsibilities 5-10
 - 5.6.4 Limitations and Exclusions 5-10
 - 5.6.5 MPSCS Responsibilities 5-11
- 5.7 On-site Response 5-11
 - 5.7.1 Description of Service 5-11
 - 5.7.2 Scope 5-11
 - 5.7.3 Inclusions 5-12
 - 5.7.4 Motorola Solutions Responsibilities 5-12
 - 5.7.5 MPSCS Responsibilities 5-12
- 5.8 Software Updates 5-13
 - 5.8.1 Description of Service 5-13
 - 5.8.2 Scope 5-13
 - 5.8.3 Inclusions 5-13
 - 5.8.4 Motorola Solutions Responsibilities 5-14
 - 5.8.5 Limitations and Exclusions 5-14
 - 5.8.6 MPSCS Responsibilities 5-14

Section 6

- Equipment List 6-1

Section 7

- Professional Services 7-1

Section 8

- Training 8-1

Section 9

- Backhaul as Service with Critical Connect 9-1
 - 9.1 MPSCS Enterprise Options (required) 9-1
 - 9.1.1 Initial Setup/One time Costs (*Totals from Sections 6 & 7) 9-1



- 9.1.2 Single Link (with Wireless Backup) + Bandwidth Option 9-1
- 9.1.3 Dual Link (2nd Fiber Line Built Out) + Bandwidth Option 9-2
- 9.1.4 Optional One Time Add-Ons 9-2
- 9.2 Available for Purchase to statewide agencies and end users: (optional)..... 9-3
- 9.3 Summary 9-5
 - 9.3.1 Annual Cost: BH+CC+WAVE+Support (Minimum vs. Maximum)..... 9-5



SECTION 1

APPLICABILITY

These Subscription Services for Critical Connect will be governed by the terms and conditions in Schedule H – Subscription Services Schedule in addition to the Standard Contract Terms in State of Michigan Contract No. 190000001544 dated October 1, 2019, as amended.

For these Critical Connect subscription services only, the Wind Down notice provision in Schedule H, Section 4.8 is changed to six (6) months' notice.

(This space is intentionally blank)



SECTION 2

SYSTEM DESCRIPTION

2.1 EXECUTIVE SUMMARY

To achieve MPSCS' goal of providing interoperability across disparate systems for the purposes of Statewide communications and beyond, Motorola Solutions is pleased to provide this proposal for ASTRO Connectivity Service (Backhaul as a Service) configured with Critical Connect. The solution provided in this proposal creates a platform by which MPSCS can establish a Statewide Enterprise Critical Connect infrastructure with the capability for expansion and use by local agencies, broadband push-to-talk providers, and multi-state regional collaborations. Critical Connect provides MPSCS centralized management of system interoperability with capability for future expansion and growth.

Motorola Solutions' ASTRO Connectivity Service (ACS) configured with Critical Connect solution enables cloud-based interoperability between different networks, agencies, and application to eliminate barriers and unify communications. This real-time exchange of voice, data, video, messaging, location, and enhanced intelligence between inter-jurisdictional agencies leads to more detailed intelligence and more informed response, regardless of device or network.

The value of Motorola Solutions' ASTRO Connectivity Service (ACS) configured with Critical Connect grows as more agencies connect, encouraging interagency cooperation through data sharing and system interoperability. For member agencies, the enhanced collaboration and increased efficiency available through Critical Connect reduce the distraction of managing a complex communication center and enable users to focus their attention and resources on critical operations.

Motorola Solutions' ASTRO Connectivity Service configured with Critical Connect enables the real-time exchange of voice, data, video, messaging, location, and enhanced intelligence between inter-jurisdictional agencies. This service package is specifically designed to encourage interagency cooperation through data sharing and system interoperability, while providing versatility, ease of use, and peace of mind.

Critical Connect requires a backhaul connection from MPSCS Site 1102 in Lansing to the Motorola Solutions Data Centers. This connection is included in this offering via Motorola Solution's ASTRO Connectivity Service. The connection is fully managed and maintained by Motorola Solutions. Please refer to Section 4 of this proposal for details of the ASTRO Connectivity Service.

The use of the features in the "Critical Connect" application is specifically dependent on the communications from the Motorola Solutions ASTRO 25 Wave Radio Gateway software to the Critical Connect software located at the Critical Connect data center. The ASTRO 25 Connectivity Service is only offered and available to ASTRO 25 systems that provide Public Safety Radio Services. The service is designed specifically to enable the use of Motorola Solutions information based applications including Critical Connect with Wave Communicator, and other cloud



and hosted applications provided by Motorola Solutions, including potential future add-ons such as Smart Connect, Smart Locate, Smart Programming. The service is not designed to support non Motorola Solutions ASTRO 25 or Application voice or data.

2.2 CRITICAL CONNECT SOLUTION DESCRIPTION

The Critical Connect solution is centered on the following elements:

- **Ease of Use** – A single, secure ISSI connection provides standards-based interoperability, reducing both the cost and complexity of interoperable PTT communications. The cloud-based interface connects multiple agencies and locations to provide a unified operating picture.
- **Flexible & Scalable** – Allows users to quickly set up and scale connections from a directory of agencies and broadband PTT carriers. Interoperable connections are easy to maintain and can grow in terms of capacity, unique connections, features, and future services, allowing the solution to quickly evolve over time.
- **Versatility** – Supports multiple types of communications, such as ASTRO 25 to ASTRO 25 communications and ASTRO 25 to carrier-integrated broadband push-to-X (talk, messaging, and mapping).

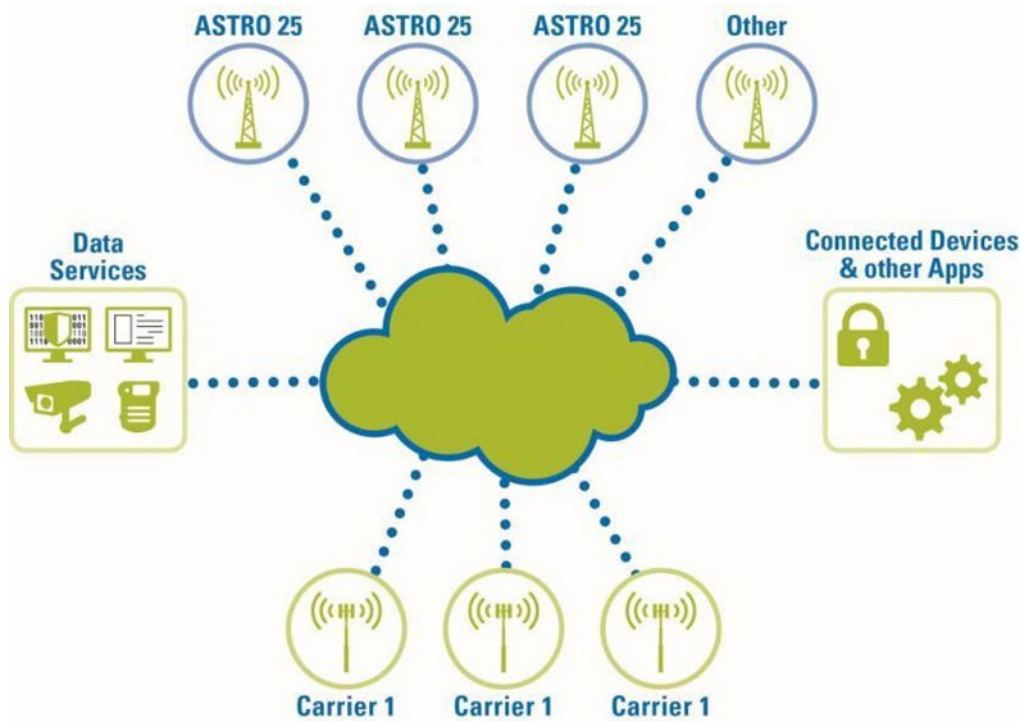


Figure 2-1: Motorola Solutions Carrier-Integrated Broadband PTT

Critical Connect grants users access to the following features to improve coordination and agency response:

- **Talkgroup Linking** – Administrators can link local and remote talkgroups to provide voice interoperability with enhanced capabilities like sharing of group IDs,



user IDs, and emergency calls and alerts. Up to eight (8) talkgroups can be linked per connection, and the type of talkgroups that can be linked include radio local and remote talkgroups, broadband PTT local, and remote talkgroups.

- Manual Roaming** – Administrators can enable manual roaming by linking home and foreign talkgroups through the Critical Connect Portal using the talkgroup linking feature. Home radio users must be programmed and allowed in the foreign systems being visited. Manual roaming requires the user to change the channel to affiliate with the foreign system.
- Automatic Roaming** – Automatic Roaming enables a radio roaming into a foreign system to continue talking with its home talkgroup without having to change channels. There is no intervention required by an administrator in the Critical Connect Portal to enable this feature. This capability is only setup and configured during Critical Connect onboarding.
- Architecture** – Critical Connect is hosted in a highly-secured, geographically separated dual cloud datacenters. All traffic leaving a customer’s premises is encrypted using AES-256.
- Redundancy** – Critical Connect offers multiple levels of redundancy. At the cloud, by default we have in-data center redundancy in addition to geo-redundancy if a data center is lost. At MPSCS Site 1102, Motorola Solutions has proposed redundant WRGs with Cryptotr units. For backhaul redundancy, Motorola Solutions proposes ASTRO Connectivity Service (ACS) that includes LTE backup for connecting to the Motorola Solutions Data Centers.

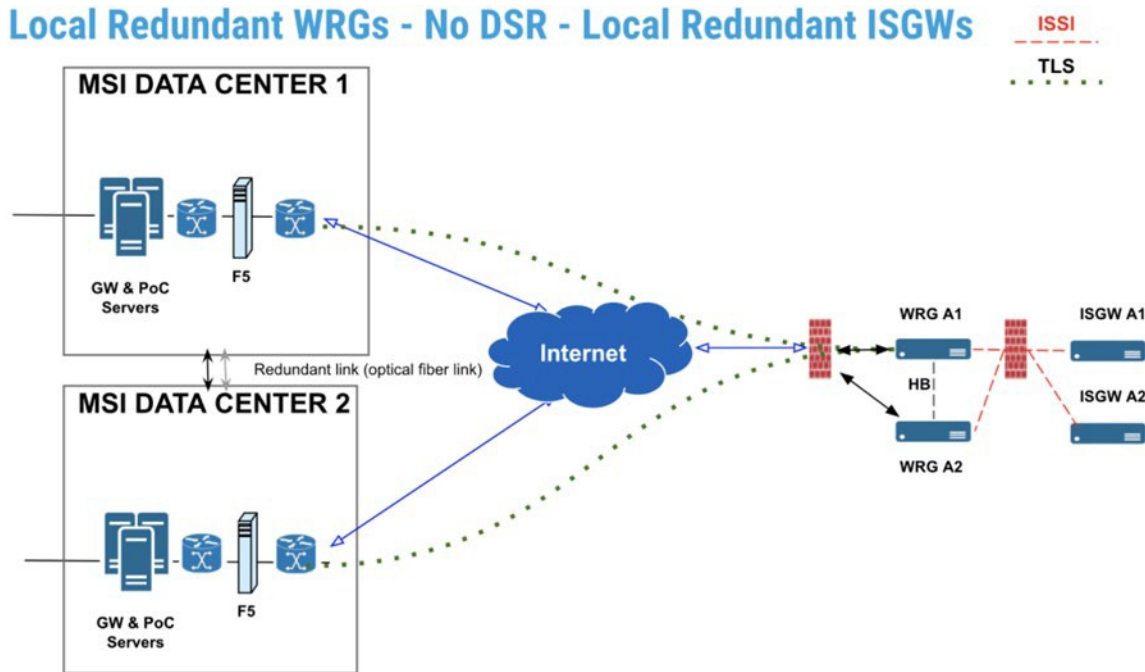


Figure 2-2: Local Redundant WRGs – No DSR – Local Redundant ISGWs



2.2.1 Sensitive Data Encryption

The ASTRO 25 system is configured with end-to-end encryption by including the WRG Cryptr at Site 1102. The Cryptr will encrypt and decrypt audio on the ASTRO 25 system. Once the traffic traverses into the Cloud through the Internetworking Firewall; however, the data is protected with FIPS-compliant validated cryptography (AES-256). Traffic from the ASTRO 25 system to the Motorola Solutions Data Center will utilize an encrypted TLS connection.

2.2.2 Restricted Traffic

The Internetworking Firewall isolates the Radio Network Infrastructure (RNI) and Customer Enterprise Network (CEN) from potentially dangerous Internet traffic. The firewall only allows sessions to the Critical Connect UGW which were initiated by the Critical Connect Site Link.

2.2.3 Secure Access

The Critical Connect Site Link connects to the Critical Connect WRG by using an encrypted link. The Critical Connect LMP also uses certificate and passphrase authentication.

On the subscriber side, the connection to the Critical Connect Site Link is also encrypted and certificate-authenticated. Each Call Grant conveys a new key, and Session Traversal Utilities for NAT (STUN) is used to detect traversals.

2.2.4 P25 ISSI (LMR-LMR Interoperability)

The Critical Connect features will support LMR to LMR communication utilizing the ISSI interface. The ISSI interface enables the home LMR systems linking or patching of talkgroups with other foreign LMR systems. Emergency Alert and Emergency Calling as well as Radio Unit IDs are all transferred between compatible systems.

Critical Connect ISSI Features

- Talkgroup linking/patching.
- Manual Roaming.
- Automatic Roaming.
- P25 Encryption with Critical Connect AES-256 keys.
- P25 Encryption End-to-End for LMR.

NOTE: Motorola Solutions is in the planning stages of P25 CAP ISSI interoperability testing Critical Connect. Testing will be conducted through accredited product testing services provided by Compliance Testing LLC. Testing is expected to be completed the first half of 2021.

2.2.5 Site Link Interface (LMR-BB)

The newly released Critical Connect Site Interface is an enhanced add-on for Critical Connect that would enable PTT functions between LMR ASTRO systems and



Broadband networks, as well as establish end-to-end connectivity for future add-on services. Critical Connect Site Interface would allow MPSCS users to:

- Send and receive private calls between broadband users and ASTRO 25 users.
- Send and receive emergency alarms between the ASTRO 25 system and broadband users.
- Group Regrouping including Supergroup Call (applicable to LMR to BB and BB to BB, not to LMR to LMR).

Using the site interface on an ASTRO 25 system, Motorola Solutions Broadband PTT subscribers can be registered as home users on the ASTRO 25 system providing a tighter integration between ASTRO and broadband PTT users. The broadband devices must be configured in the Provisioning Manager. The site interface offers scalable dynamic re-grouping (i.e., super-grouping LMR to BB and BB to BB), talkgroup priority controls, and private calling for home broadband PTT subscribers. Just as with ISSI, this connection is encrypted End-to-End with the use of the Cryptr unit with AES and the WRG to UGW is encrypted through TLS.

An LMR Multicast Proxy (LMP) is added to the Zone Core servers to convert between unicast (for the cloud) and multicast (for the P25 radio system) between the Zone Controller and the Universal Gateway in the cloud.

2.2.6 **ASTRO Connectivity Service configured with Critical Connect Capacity**

A main and redundant Wireless Radio Gateway (WRG) has been proposed. The WRG supports 50 simultaneous LMR to LMR (ISSI) talkgroup calls. The WRG can be expanded by adding up to three (3) more virtualized WRGs (installed on the proposed WRG server) to support a total of 200 simultaneous LMR to LMR (ISSI) talkgroup calls. Security Update Service for WAVE is in development; target release is second quarter 2021.

Site Link Interface supports up to 2000 Broadband subscribers per Virtualized Wave Radio Gateway. Additionally, Land Mobile Proxies (LMPs) have been included to support Broadband to LMR calls. The LMPs are installed on the existing Core VMS servers, VMS01 and VMS02. One (1) LMP is included to support 27 simultaneous Broadband to LMR (FDMA) calls or 36 simultaneous Broadband to LMR (TDMA) calls. Up to four (4) LMPs can be deployed on the system for a total of 108 simultaneous Broadband to LMR (FDMA) calls or 144 simultaneous Broadband to LMR TDMA calls or a combination of both. The additional LMPs would be installed on VMS07 and VMS08 servers which are included.

2.2.7 **Critical Connect Portal**

Through the Critical Connect portal, users have access to a variety of management tools and capabilities, as well as a map of internal and external talkgroups—different types of talkgroups, such as ASTRO 25 radio and broadband, are supported. Users have the ability to remove or reject pre- approved talkgroups as necessary.

Through the Critical Connect portal, Motorola Solutions' Link Manager enables



interoperability across broadband PTT talkgroups and LMR talkgroups, providing secure, web-based access to broadband talkgroups and LMR talkgroups that are part of an agency’s configuration. Users can dynamically link one or more broadband and LMR talkgroups (up to eight talkgroups per connection or tile). The Critical Connect Portal also allows users to share a talkgroup outside of their agency to other agencies, using an “Invite-Approve-Reject” model in these situations. Talkgroups shared outside of an agency are viewed as external talkgroups. Agency administrators can create a talkgroup link across internal as well as external agency talkgroup. See Figure 2-6.

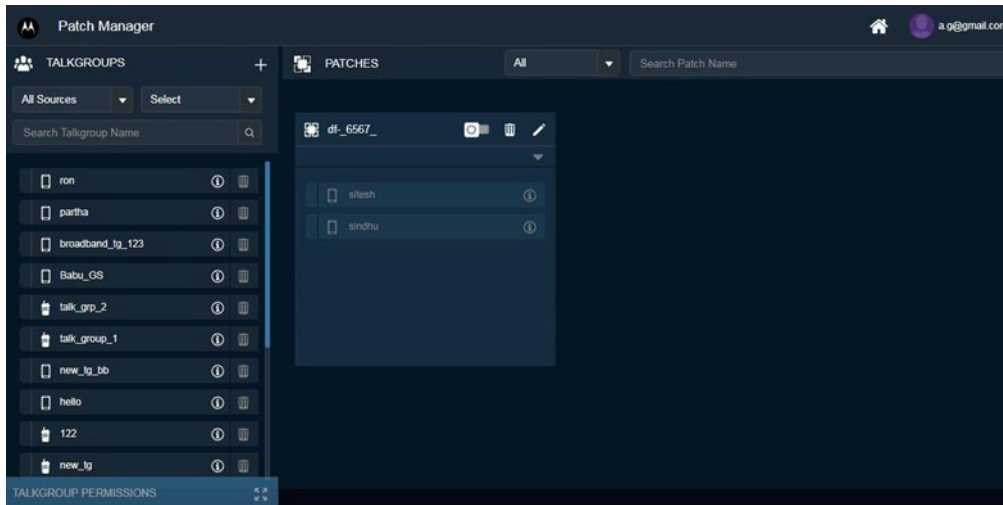
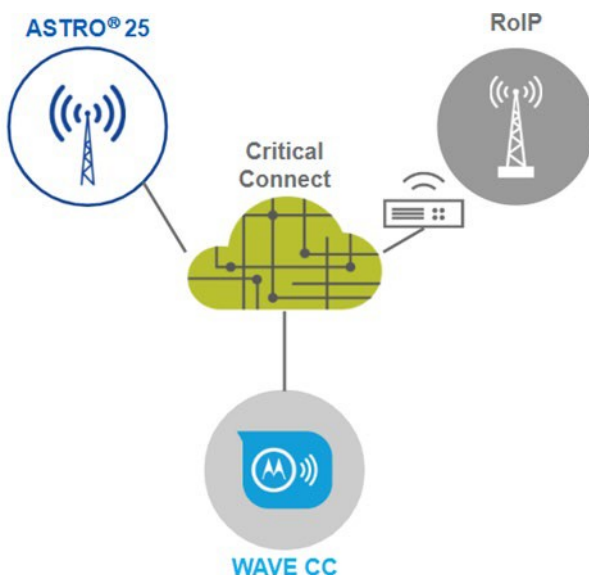


Figure 2-6: Critical Connect Portal’s Patch Manager Screen

2.3 ADDITIONAL CRITICAL CONNECT INTERFACES

The Critical Connect platform is equipped with multiple interfaces allowing it to bridge different disparate radio systems and Motorola Solutions’ Broadband PTT solutions. Land Mobile Radio users are able to connect to multiple different types of systems across multiple boundaries with one connection to Critical Connect.

2.3.1 Radio-over-IP (RoIP) Link



Included in the premium package, is the Radio-Over-IP (RoIP) access. RoIP allows an ASTRO 25 customer using Critical Connect to link non-standard based radio systems such as analog radio sites, non-ASTRO trunked and conventional sites, and DMR type systems with their home radio talkgroups.

RoIP provides basic voice and PTT control (COR signaling) that is converted into an accessible talkgroup by Critical Connect and can be linked (patched) to other talkgroups.



To enable this feature, Critical Connect customers must license the RoIP link feature and procure the RoIP gateways from Cubic Vocality or one of its dealerships.

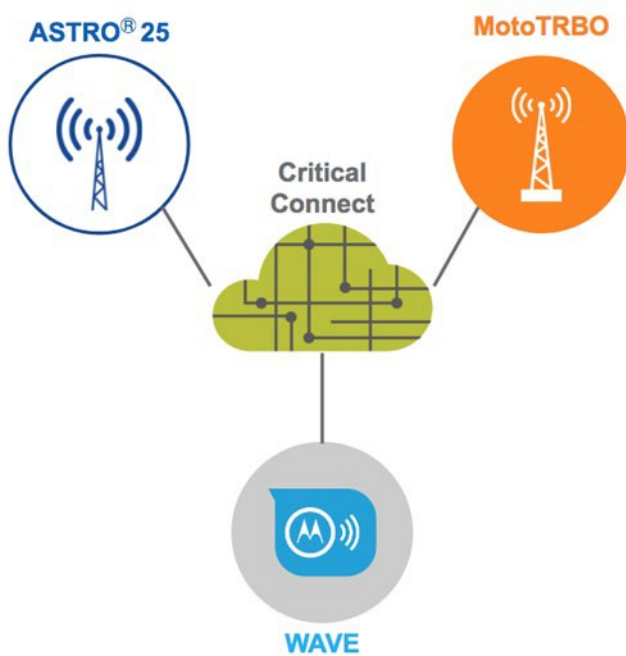
Critical Connect uses third-party RoIP gateways to support this functionality. Today, we use the Cubic Vocality RoIP Gateway. Using Cubic’s Vocality RoIP gateway, users can connect a donor radio or control station’s 4-wire* interface and convert it into a secure IP-based radio talkgroup that will show up in the Critical Connect Portal as another talkgroup.

The Vocality RoIP gateway uses a secure TLS AES-256 connection to Critical Connect, providing a secure IP connection for radio communications. Once the talkgroup is available in the portal, it can be linked with other resources such as P25 talkgroups and/or Broadband PTT talkgroups.

With the Vocality RoIP gateway, up to four talkgroups per gateway can be configured to connect to Critical Connect.

* Motorola Solutions recommends using donor radios or control stations that provide COR signaling for the best user experience. Most mobile radios do this but typically portable radios do not provide a COR signal.

2.3.2 MOTOTRBO Link



Included in the premium package is MOTOTRBO Link access. MOTOTRBO access grants ASTRO 25 customers of Critical Connect the access to radio users of MOTOTRBO systems like K-12 school systems, universities, utilities and public civilian systems relying on this technology. Critical Connect customers will be able to link P25 and MOTOTRBO talkgroups easily through the use of the Critical Connect Portal. This connection can also be expanded to include Broadband PTT.

The MOTOTRBO link interface is compatible with several different flavors of MOTOTRBO such as Capacity Plus, Link Capacity Plus, Capacity Max and IP Site Connect.

To enable this feature, Critical Connect customers must license the MOTOTRBO link feature and MOTOTRBO customers must procure the TRBO WRG gateway through the “bring your own gateway” offered by commercial dealers.

2.3.3 Data Interface

Critical Connect leverages the ASTRO 25 IMW interface to bring additional bridged data capabilities to APX, APX NEXT and Motorola Solutions’ broadband PTT



devices. This interface to your existing IMW or the redundant IMW is included and will provide you with the ability to add data capabilities described below. These data capability services are available for use through CAD and dispatch applications*.

- Text messaging
- Presence*
- Affiliation*
- Location services*

*Upcoming 2021 services and applications.

Presence and Location licenses for the IMW are required as the agencies are added. Costs to add these licenses would be quoted at the time, and the costs are dependent on the number of agency users being added (one license per user). Location services requires the transport and display of locations coordinates to end user agency's mapping application. CAD or Command Central Aware are two applications that are available for displaying location. Costs for each agency are dependent on their mapping application and require a REST interface to the IMW.

APX Next and Broadband devices will report their location over the LTE network into the Cloud. APX radios reporting their location over the ASTRO 25 radio system would require Enhanced Data operation on the ASTRO 25 radio system to support location reporting.

2.3.4 Gateway-to-Gateway Interface

Motorola and MPSCS will discuss the viability of establishing a gateway-to-gateway interface in the future, with the required network security stack, to support connectivity to Critical Connect by the locals without requiring dedicated ACS connections during the DDP process.

2.4 WAVE PTT SOLUTION OVERVIEW

To offer greater flexibility and allow agencies to implement a device-agnostic and carrier-independent policy for push-to-talk (PTT) communications, Motorola Solutions offers WAVE integration to Critical Connect customers.

As part of the implementation of this solution, Motorola Solutions will host a workshop for collaboration with MPSCS to define the customer onboarding and migration process.

WAVE is a cloud-based solution that enables interoperable PTT across devices, networks, and locations. Users receive instant, reliable PTT that extends communications beyond the coverage provided by an LMR system. With easy installation and straightforward provisioning of new users, WAVE can easily scale and adapt as needs evolve. Costs are kept predictable with a low monthly subscription, offering reliable and budget-friendly unified communications. This simplified pricing structure consists of a monthly, per-user plan with broadband and LMR interoperability.

WAVE enhances your Critical Connect solution with the following benefits:

- Enables ASTRO 25 to broadband PTT WAVE communications, leveraging the



latest broadband LTE and Wi-Fi nationwide coverage to support varying communications needs.

- Eliminates communication barriers between agencies by enabling virtual connections, as communication needs arise.
- On-demand fleet-maps provide flexible communications that adapt to changing needs.
- Critical Connect offers inter-agency group voice communication between ASTRO 25 radios and broadband mobile devices.

WAVE offers users the following capabilities:

- **Group Call** – Talkgroup participants (including both LMR and WAVE users, WAVE-only users, and LMR-only users) can make group calls using any WAVE application. Users select the talkgroup, push-to-talk, and the talkgroup can hear the speaker's transmission and can reply. Talkgroups and assigned participants are created and managed by the WAVE Central Administration Tool.
- **Individual Private Call** – Make private calls between two WAVE users. A user selects the person they wish to call from a contact list available within the application and can communicate with a simple button press.
- **Text Messaging** – Send and receive group text messages with other WAVE users in a talkgroup.
- **Multimedia Sharing** – Share images or videos from the gallery or directly from the camera. Users can share with other users or a group, and can view received videos and photos, play or save to their device. Users' history saves media to view when they login. Live Streaming available at an additional monthly rate.
- **Location** – Users can see where WAVE group members are located on a map.
- **Voice Message Pre-Recorded or Record-and-Send** – Users can record a message that can be sent to a group or to a contact. Voice messages can be played back by users at any time.
- **Persistent Threaded History on Client** – Users can see the history of text messages and PTT events for group or private calls even if they log out and log back in. Events that happened while they were logged out will be pushed down to the client so that they are caught up.
- **PTT from Lock Screen** – Users can quickly PTT from a device's lock screen without having to unlock the device or go through the application. This is exclusive to Android devices.
- **Headset Integrations** – Wired or Bluetooth headsets can be used to respond hands-free in any situation.

WAVE users engage with two different, interoperable clients: the WAVE Mobile Client and WAVE Dispatch Client. Each client grants access to enhanced WAVE PTT features, as shown in the table below.

(This space is intentionally blank)



Table 2-1: Enhanced WAVE PTT Features

WAVE Mobile Application	WAVE PTT Plus	WAVE Dispatch Application	WAVE Dispatch Plus
PTT (Private and Group Calling). Presence and Alerts. Secure Messaging and Multimedia. Location & Mapping Services. Administrator and User-managed Contacts / Groups. Integrated Web-based Broadband Dispatch Console.	PTT (Private and Group Calling). Presence and Alerts. Secure Messaging and Multimedia. Location & Mapping Services. Administrator and User-managed Contacts / Groups. Integrated Web-based Broadband Dispatch Console. Emergency Services. User Check and Monitor. Ambient and Discreet Listening. Large Talkgroup Size (3000).	PTT (Private and Group Calling). Presence and Alerts. Secure Messaging and Multimedia. Location & Mapping Services. Administrator and User-managed Contacts / Groups. Integrated Web-based Broadband Dispatch Console.	PTT (Private and Group Calling). Presence and Alerts. Secure Messaging and Multimedia. Location & Mapping Services. Administrator and User-managed Contacts /Groups. Integrated Web-based Broadband Dispatch Console. Emergency Services. User Check and Monitor. Ambient and Discreet Listening. Large Talkgroup Size (3000). Dynamic Area Talkgroups. MC Streaming Video.

(This space is intentionally blank)

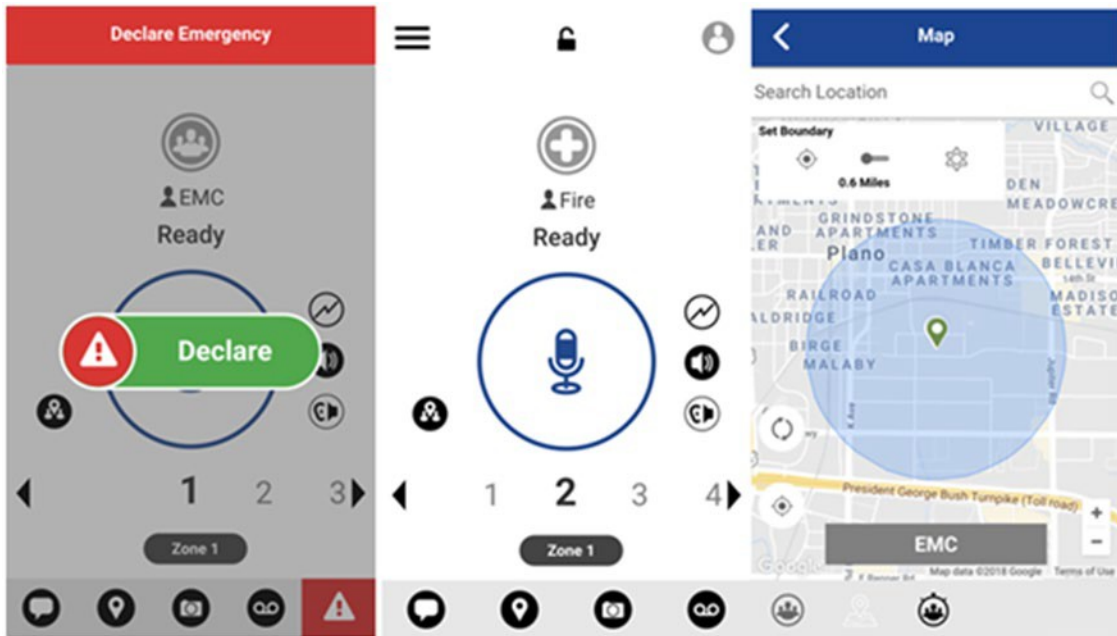


Figure 2-7: Examples of PTT Call Ready Radio Screen, Active Emergency, and Location Services Screen

WAVE is compatible with Android and iOS devices over 3G, 4G, and Wi-Fi networks globally, providing hardware flexibility to fit different customer setups.

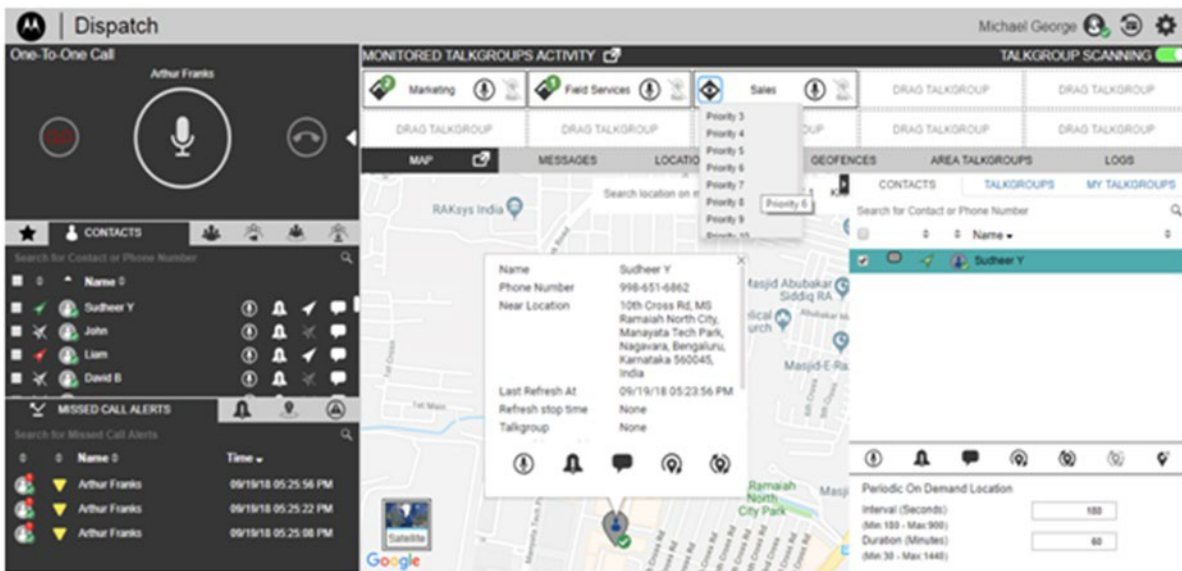


Figure 2-8: Example of the WAVE Dispatch Screen



2.4.1 WAVE Administration Portal

WAVE’s Central Administration Tool (CAT) helps administrators manage user contacts and talkgroups. The WAVE Administration Portal allows users to manage PTT user profiles and permissions, talkgroups, and external users.

- PTT Users Management:** Allows users to manage the PTT user profile such as name, email ID, and permission type.
- Talkgroups Management:** Allows users to manage talkgroups including, assigning avatar, talkgroup scanning, supervisory override, permission to the talkgroup members for call initiation, and receive and in call accessibility. There are three types of talkgroups that users can manage: standard, dispatch, and broadcast groups.
- External Users Management:** Allows users to manage users external to the corporation.
- Interop Connections Management:** Allows users to manage the connections between Critical Connect and PTT.
- User Sets:** Allows users to manage the user sets to PTT Users, Talkgroups, or Integrated Users.

Name	Facilities	Talkgroup Type	Dispatch	Member
Name	Facilities	Talkgroup Type	Dispatch	Member 53
Name	Field Service	Talkgroup Type	Dispatch	Member 99
Name	Managers	Talkgroup Type	Standard	Member 47
Name	Urgent Response	Talkgroup Type	Dispatch	Member 6
Name	Zone 1	Talkgroup Type	Standard	Member 4
Name	Zone 2	Talkgroup Type	Standard	Member 4
Name	Zone 3	Talkgroup Type	Standard	Member 28

Figure 2-9: Example of the WAVE CAT Screen

(This space is intentionally blank)



2.5 INFRASTRUCTURE UPDATES

Further changes are required at the UNC and the Provisioning Manager to implement Critical Connect. A summary of the required changes are listed below. For a detailed step by step explanation of the procedures see Addendum 2.

- Configure the WAVE Oncloud System Under Foreign System Configuration.
- Configure the Foreign Systems Configuration in the UNCW.
- Configure the Registration Lifetime In the UNCW.
- Configure the Foreign System Frequency Band Plan in the UNCW.
- Configure the Foreign Site Configuration in the UNCW.
- Configure Adjacent Sites.
- Approve Job in UNC.
- Verify and Distribute from The Provisioning Manager.
- Distributing Home Zone Maps and Conventional Home Zone Maps.
- Configure System DNS for The Foreign System IP On The Active Director.
- Verify Connectivity Between ISGW and The Foreign System.
- Verify DNS Resolution.
- Subscriber Programming.

2.6 RESPONSIBILITY MATRIX

IE = Motorola Integration Engineer

Market Team = Motorola Market Team

ST = Motorola System Technologist

Responsibilities	Team
Create and Maintain Project Workbook.	IE
Assign Market PM as single point of contact.	Market Team / MPSCS
Provide Customer Support representatives with the proper information to assist in Tier 1 support issues.	MPSCS
Create Deployment Schedule.	IE / Market Team
Schedule Weekly Project Calls.	IE
Verify VMS for LMP installed.	Field Eng / ST
Verify Internetworking Firewall.	Field Eng / ST
Order HW/SW/License required.	Market Team
Design and collaborate with MPSCS on a Network plan and IP schema for CC deployment.	Field Eng / ST
Complete Field Questionnaire and Config workbook.	Field Eng / ST
Provide a dedicated VLAN for Critical Connect off of existing WAVE5000 subnet.	MPSCS
Update LAN Switch config.	Field Eng / ST
Remove existing demo WRG server and Cryptr at site 1102 and relocate to the Lab with assistance from MPSCS.	Field Eng / ST / MPSCS



Responsibilities	Team
WRG and Cryptr Physical Install / cabling; Qty 2.	Field Eng / ST
Additional Rack Unit space will be needed for accommodating the ACS equipment. Adequate space is available for additional equipment at MPSCS Site 1102.	MPSCS
Provide adequate electrical power in proper phase and voltage at sites.	MPSCS
Execute Critical Connect LMP and Internetworking Firewall Installation MOP.	Field Eng / ST
Load Key to Cryptr.	Field Eng / ST
Provide Remote Access to WRG Server for IE Team.	Field Eng / ST
Configure Qty (2) WRGs.	IE
Create a WAVE OnCloud account and provision WAVE OnCloud users.	IE
Provision Test TGs and Subscribers for Functional Test / ATP.	IE
Create Patching for Functional Test / ATP.	IE
Verify WRG - LMP Integration.	IE / Field Eng / ST
Perform Functionality Test.	IE / Field Eng / ST
Perform ATP Dry Run.	IE / Field Eng / ST
Execute ATP with MPSCS.	IE / Field Eng / ST / MPSCS
Obtain the list of TGs and Users from MPSCS.	Market Team / MPSCS
MotoPatch	MPSCS
Provision TGs and Users for close out.	IE
Obtain the list of Portal Admin users from MPSCS.	Market Team / MPSCS
Provision Portal Admin users.	IE
Provide navigation resources for on-boarding process.	IE / MPSCS / PM
Provide training for Corporate App Tool (CAT), Patch Portal and WAVE app usage.	IE / MPSCS
Transition to CSM / Support Team.	Market Team

(This space is intentionally blank)



SECTION 3

CRITICAL CONNECT - STATEMENT OF WORK FOR INSTALLATION AND ONBOARDING

This Statement of Work (SOW) is an integral part of the Subscription Services Agreement for the Critical Connect Services entered into by Motorola Solutions, Inc. (Motorola Solutions) and MPSCS ("Agreement") and will be governed by the terms and conditions in the Agreement. If there is a conflict between the terms of the Agreement and the terms of this SOW, the terms of this SOW will govern.

This SOW describes the activities required in deploying a redundant enablement server (also called a Critical Connect WAVE Radio Gateway Server ["WRG Server"]) on an ASTRO 25 customer premises, connecting the WRG Server to Critical Connect, and connecting the WRG Server to the ISSI Gateway ("ISGW")/ASTRO 25 Core as well as the redundant RNI-DMZ firewall connections and the HA core setup. This SOW is an integral part of the Subscription Services Agreement for interoperability services.

3.1 CONTRACT

3.1.1 Contract Award (Milestone)

MPSCS and Motorola Solutions execute the Agreement and both parties receive all the necessary documentation.

3.1.2 Contract Administration

Motorola Solutions Responsibilities

- Assign a Project Manager as the single point of contact with authority to make project decisions.
- Assign resources necessary for project implementation.
- Schedule the project kickoff meeting with MPSCS.

MPSCS Responsibilities

- Assign a Project Manager as the single point of contact with authority to make project decisions.
- Assign other resources necessary to ensure completion of project tasks for which MPSCS is responsible.

**Completion Criteria**

- Both Motorola Solutions, Inc. and MPSCS assign all required resources.
- Project kickoff meeting is scheduled.

3.2 CONTRACT DOCUMENT REVIEW

3.2.1 Review Contract Document

Motorola Solutions Responsibilities

- Meet with the MPSCS project team.
- Review SOW, Project Schedule, and Acceptance Test Plans, and update the contract documents accordingly.
- Establish and review interfaces supplied by Motorola Solutions that define the connection between the MPSCS ISGW (ASTRO 25 Core), WRG Servers, and Critical Connect in Motorola Solutions data center.
- Submit network topology and configuration to MPSCS for approval.

MPSCS Responsibilities

- The MPSCS's key project team participants attend the meeting.
- Make timely decisions, according to the Service Deployment Project Schedule.

Completion Criteria

- Agreement between Motorola Solutions and MPSCS on updates to contract documentation.
- Updated contract documentation, which may include updated SOW, Project Schedule, Network Topology, and Acceptance Test Plans.
-

3.3 ORDER PROCESSING

3.3.1 Process Equipment List

Motorola Solutions Responsibilities

- Validate Equipment List by checking for valid model numbers, versions, compatible options to main equipment, and delivery data.
- Create Ship Views, to confirm with MPSCS the secure storage location(s) to which the equipment will ship.
 - Ship Views are the mailing labels that carry complete equipment shipping information, which direct the timing, method of shipment, and ship path for ultimate destination receipt.
- Create equipment orders.
- Reconcile the equipment list(s) to the Contract.
- Procure third-party equipment if applicable.

MPSCS Responsibilities

- Approve shipping location(s).



Completion Criteria

- Motorola Solutions will verify that the equipment list contains the correct model numbers, version, options, and delivery data.

3.3.2 Install Enablement Server (WRG) Server Equipment

Motorola Solutions Responsibilities

- Provide for the installation of redundant WRG Servers and associated network equipment that will interface with the following network connections:
 - ISGW Gateway and External Critical Connect Servers.
- All equipment will be installed employing a standard of workmanship consistent with Motorola Solutions R56 installation standards and in compliance with applicable National Electrical Code (NEC), EIA, Federal Aviation Administration (FAA)/Transport Canada, and FCC standards and regulations/Industry Canada.
- Remove existing WRG Server and Crypttr box from demo equipment at 1102 and relocate to the Lab for MPSCS to use.
- Receive and inventory all equipment.
- Bond the supplied equipment to the existing site ground system in accordance with Motorola Solutions R56 standards.
- Coordinates the receipt of the equipment with MPSCS's designated contact, and inventory all equipment.
- Provide the R56 requirements for space, power, grounding, HVAC, and connectivity requirements at each site.
- Motorola Solutions will perform installation tasks on site as outlined in the Method of Procedures (MOP).
 - NOTE: Manual and Automatic Roaming functionality requires additional configuration through the ASTRO provisioning manager that is not covered under the Critical Connect onboarding services.
 - ◆ MPSCS will use the provisioning manager and be able to implement the required configuration updates with guidance from the Motorola Solutions' ASTRO team. These necessary changes were addressed in the above System Description.

MPSCS Responsibilities

- MPSCS agrees to provide rack space and power at MPSCS Site 1102 site location as part of the deployment of the Critical Connect Service.

Rack & Power Requirements	QTY	R/U	Depth	Power	Plug
HP Server	2	2	48"	15A/Unit	NEMA 5-15p
Crypttr	4	1	8"	.3A/Unit	NEMA 5-15p

- NOTE: Additional Rack Unit space will be needed for accommodating the ACS equipment. Motorola Solutions assumes adequate space is available for additional equipment at MPSCS Site 1102.

Additional MPSCS Responsibilities

- Provide secure storage for the Motorola Solutions provided equipment at a location central to the site.



- Coordinate the receipt of the equipment with Motorola Solutions and inventory all equipment.
- Provide access to the sites, as necessary.
- Provide adequate electrical power in proper phase and voltage at sites.
- Confirm that there is adequate utility service to support the new equipment and ancillary equipment.
- Ensure that each site meets the R56 standards for space, grounding, power, HVAC, and connectivity requirements.
- Provide site owners/managers with written notice to provide entry to sites identified for Motorola Solutions personnel.
- Provide IT support, as needed, during project implementation.
- MPSCS is responsible for providing broadband devices with broadband service and ASTRO 25 radios for Functional Acceptance Testing.
 - NOTE: Subscriber radio programming and services are not included. If required, a separate quote can be provided upon request.
- MPSCS is responsible for assigning a representative to witness system acceptance testing.

3.4 FUNCTIONAL ACCEPTANCE TESTING

Motorola Solutions, Inc. will provide an Acceptance Test Plan (ATP) based upon the Critical Connect Services being onboarded. The ATP will outline the testing procedures and acceptance criteria required to demonstrate 'normal operation' of the Critical Connect services.

3.4.1 Perform Functional Testing

Functional acceptance testing will occur in four(4) phases in a series of agile sprints as follows:

- Phase 1 – LMR to LMR functional acceptance testing using the P25 ISSI connection described in section 2.2.4.
- Phase 2- LMR to broadband functional acceptance testing using the Site-Link Interface described in section 2.2.5.
- Phase 3 – Broadband to functional acceptance testing.
- Phase 4 – Aware client functional acceptance testing.

Motorola and MPSCS will determine the optimal installation plan for the necessary equipment and network modifications to support the functional acceptance testing for each phase during the DDP process.

Functional acceptance testing for Phase 1 will include testing of the redundant wireless network link to ensure that link performs as expected with respect to latency and timing.



Motorola Solutions Responsibilities

- Motorola Solutions will perform Functional Acceptance Testing of the procedures outlined in the ATP.

MPSCS Responsibilities

- Witness the functional Acceptance Testing.

Completion Criteria

Successful completion and MPSCS approval of the functional testing

- A Field Functional Test will be performed after completing the on-site installation and setup of the WRG Servers, and necessary configuration for Broadband to ASTRO 25 and ASTRO 25 to ASTRO 25 Interoperability.

3.4.2 System Acceptance Test Procedures (Milestone)

- Successful demonstration of functional tests outlined above to the MPSCS users participating in the testing will constitute successful system acceptance by the MPSCS. The acceptance criteria is 100% passing of the tests outlined in the ATP, inclusive of specific tests to ensure CAP compliance, and witnessed by MPSCS.

NOTE: ATP must be scheduled within the month following the successful implementation of Critical Connect. Failure to execute the ATP within this timeframe will constitute successful system acceptance by the MPSCS.

Dependencies and Assumptions

- MPSCS responsibilities are outlined in this SOW above. All MPSCS responsibilities must be met after the contract signing and prior to the start of the installation on the MPSCS site.
- If any of the MPSCS responsibilities are not met, start and/or completion of the installation activity and service start date would be delayed. Motorola Solutions, shall not be responsible for any delays or non-performance caused by MPSCS failing to meet MPSCS responsibilities.
- If extraordinary delay is caused in start and/or completion of installation and setup of the site equipment is caused because of not meeting any of the MPSCS responsibilities, modification of implementation schedule will be required.

3.5 PROJECT SCHEDULE

Motorola Solutions understands the importance and priority for MPSCS to have the Critical Connect solution operational for their public safety customers. It is also in Motorola Solutions' best interest to move as quickly as possible in reaching a successful deployment of the proposed solution. A final schedule will be reviewed and agreed upon jointly with the MPSCS team at the Detailed Design Review.



SECTION 4

CRITICAL CONNECT - STATEMENT OF WORK FOR REQUEST FULFILLMENT

4.1 AGREEMENT

This Statement of Work (SOW) is an integral part of the Subscription Services Agreement for the Critical Connect Services entered into by Motorola Solutions, Inc. (Motorola Solutions) and MPSCS (“Agreement”) and will be governed by the terms and conditions in the Agreement. If there is a conflict between the terms of the Agreement and the terms of this SOW, the terms of this SOW shall prevail.

4.2 REQUEST FULFILLMENT BY SERVICE DESK

Request Fulfillment is a service, as defined herein, available to the MPSCS with a Critical Connect subscription managed by Motorola Solutions. Request Fulfillment enables users of Critical Connect to request support services as set out in this SOW (“Fulfillment Services”). MPSCS or its authorized Critical Connect users (“Users”) may request the Fulfillment Services through Request Fulfillment.

The objectives of Request Fulfillment Service are as follows:

- Provide a mechanism for users of the Critical Connect Services to request and receive Fulfillment Services set forth in this SOW.
- Provide information to the MPSCS and Users about the availability of Fulfillment Services and the pre-defined approval and qualification procedures for obtaining them.
- Assist with general information or questions.

4.2.1 Service Desk

Motorola Solutions has established a service desk to monitor, escalate, provide dispatch assistance, and fulfill service requests (“Service Desk”).

The Service Desk provides a single point of contact for Users of Critical Connect on a day-to-day, 24x7 basis. The Service Desk handles all incidents and service requests, using specialized, proprietary software tools and methodologies to log and manage all such events.

The primary goal of the Service Desk is to provide incident resolution and restoration of service to ‘normal operation’ as demonstrated during the functional acceptance testing. Restoration of service may involve fulfilling a service request or handling



relevant queries about a service process that is needed to allow Critical Connect services to return to normal operation.

The Service Desk contributes to an integrated service management approach through:

- Answering MPSCS or User phone requests regarding Critical Connect service issues in accordance with the timeline metrics set forth in the Customer Support Plan (CSP). The CSP is an integral part of this SOW and once agreed upon by the parties, will be automatically incorporated into this SOW.
- Responding to phone calls regarding Fulfillment Service, Critical Connect, and/or security matters relating to the Fulfillment Services.
- Receiving and responding to emails on matters regarding reported issues or requested services.
- Monitoring and receiving MPSCS or User incident tickets.
- Verifying, analyzing, and validating reported issues.
- Performing initial impact analysis of reported incidents.
- Opening, issuing, or updating corresponding incident tickets, as appropriate.
- Escalate to the next level of support within the period of time set forth in the CSP, if required.

4.2.2 Fulfillment Service Process Descriptions

Request Fulfillment utilizes the following process:

- Receive Service Request – Requests are submitted through a pre-defined process agreed upon by Motorola Solutions and the MPSCS in the Customer Support Plan (CSP). The CSP is an integral part of this SOW and once agreed upon by the parties will be automatically incorporated into this SOW.
- Logging and Validation – Service Requests are logged with a Service Request record created at the Service Desk with relevant information and a description of the request.
- Categorization and Prioritization – Service Requests are categorized by type and nature, and prioritized in relation to other new and existing requests to determine the sequence in which they will be fulfilled. Priority is determined based on severity, level of effort, benefit to the organization and urgency to the requestor.
- Review and Authorization – Service Requests are reviewed for categorization, prioritization, and User profiles to determine the correct level of agreed upon authorization. Requests also may have functional and/or financial impacts which are factors considered during authorization.
- Execution and Closure – Service Requests are routed to the appropriate fulfillment team. The fulfillment team follows documented procedures for fulfilling the request. Certain requests, such as questions or inquiries, may be completed by the Service Desk, acting as first-line support, while other Service Requests are forwarded to specialist groups and/or suppliers for fulfillment.

4.2.3 Roles and Responsibilities

Motorola Solutions Responsibilities

- Make available all Service Desk contact options and contact information.



- Modify existing Customer Support Plan.
- Respond to requests in accordance with the pre-defined severity levels set forth in the CSP.
- Log, validate, categorize and prioritize all received requests.
- Manage and fulfill service requests.

MPSCS Responsibilities

- Provide all relevant and accurate information requested by Motorola Solutions in order to develop a CSP or modify an existing one.
- Collaborate with Motorola Solutions to document service request and approval process.
- Ensure Users are notified about the request process and required authorizations.
- Contact Motorola Solutions, as necessary, with service requests.
- Ensure appropriate requests are pre-authorized, as required.
- Cooperate with Motorola Solutions and perform all acts and provide all information in a timely manner that is necessary to enable Motorola Solutions to respond to service requests.
- Support closure of request as requested by the Service Desk.
- Obtain any third-party consents for Motorola Solutions to provide the FulfillmentService, if applicable.

4.3 CRITICAL CONNECT TECHNICAL SUPPORT

This SOW introduces the Technical Support service which is part of Service Delivery Management for Critical Connect. The objective of Technical Support is to provide administrative support of the Critical Connect Service.

4.3.1 Fulfillment Service Description

Motorola Solutions Critical Connect Technical Support provides support calls for technical requests and incidents from authorized points of contact from MPSCS to help MPSCS in resolving issues.

Technical Support standard operating hours are 8/5/5, Monday through Friday. Calls can be made to the Motorola Solutions Help Desk 24x7; however, only Severity 1 (total service outage) issues will be addressed by Technical Support outside of standard operating hours. Please refer to the CSP for severity definitions and associated target service response windows.

4.3.2 Roles and Responsibilities

Motorola Solutions Responsibilities

- Provide Technical Support 8/5/5, Monday through Friday.
- Receive Technical Support request at the Service Desk and categorize.
- Verify access request for User authenticity and the legitimate right to access the service being requested.
- Define problem based on the following parameters:
 - Critical Connect Server Connection issue.



- Internet Connectivity verification.
- Password Reset.
- Verify with MPSCS the proper functioning of the Critical Connect service based on troubleshooting steps performed.

MPSCS Responsibilities

- Designate authorized personnel as Administrators.
- Reference the CSP for appropriate severity levels and call routing procedures.
- Provide Motorola Solutions Customer Support representatives with the proper information to assist in Tier 1 support issues.
- MPSCS to provide a dedicated VLAN for Critical Connect off of the existing WAVE5000 subnet.
- Verify with Motorola Solutions the proper functioning of Critical Connect based on troubleshooting steps performed.
- Obtain third party consents, as necessary for Motorola Solutions to provide the Fulfillment Service.

4.4 INFRASTRUCTURE HARDWARE REPAIR

Motorola Solutions provides a hardware repair service for identified infrastructure equipment supplied by Motorola Solutions. A Motorola Solutions authorized Repair Depot manages the repair of Motorola Solutions supplied equipment, as well as coordinating the equipment repair logistics process. The Critical Connect application software will reside on redundant HP DL380 servers. Any hardware related support issues with the HP server will be directed to HP via the Motorola Solutions SSC Service Desk (Call Center Operations Team). Each HP DL380 server will have (2) Motorola Crypters (used for encryption on both ISSI and SLI).

4.5 CRITICAL CONNECT ON-SITE SUPPORT

Motorola Solutions' On-Site Support service is triggered during the initial support process if it is determined that an on-site technical representative is needed to access error logs or address issues with the Critical Connect WAVE Radio Gateway (WRG) hardware. The Motorola Solutions On-Site Support service provides incident management and technical service support to enable on-site incident resolution relating to the Critical Connect WAVE Radio Gateway (WRG) hardware. The On-Site Support is delivered in conjunction with a third-party services provider (On-Site Service Provider). The On-Site Service Provider is responsible for providing On-Site Support through the On-Site Support to ensure strict compliance with committed response and resolution times outlined in the CSP.

4.5.1 On-Site Support Description

The Motorola Solutions Service Desk will dispatch an On-Site Service Provider and then provide support to maintain contact with the On-Site Service Provider until system restoration.

Once dispatch is issued and received, the On-Site Service Provider will respond to the MPSCS location based on pre-defined severity levels set forth in the CSP.



Motorola Solutions Technical Support will provide support and maintain contact with the On-Site Service Provider until system restoral and incident closure occurs. The On-Site Service Provider will be required to provide incident status updates on a predefined basis to allow tracking of incident status.

As part of the On-Site Support service delivery, a detailed On-Site Support service process will be designed and developed according to MPSCS' needs and policies and documented in the CSP. The On-Site Support service process provides the required procedures to ensure standardized methods are used both reactively and proactively to resolve deviations from normal operations.

4.5.2 Scope

On-Site Support is available in accordance with Severity Level Definitions and Response Time Commitments listed in the CSP.

4.5.3 Roles and Responsibilities

Motorola Solutions Responsibilities

- Respond to dispatch request as required by the On-site Support Service process.
- Ensure the required service personnel have access to the MPSCS sites as needed.
- Servicer will perform the following on-site activities:
 - Run diagnostics on the server or network equipment.
 - Replace defective server or network equipment as required.
 - On-site servicer ensures that faulty server or network equipment is sent for repair with associated Return Merchandise Authorization (RMA).
 - Provide materials, tools, documentation, physical planning manuals, diagnostic/test equipment, and any other requirements necessary to perform the maintenance service.
 - If a third-party vendor is needed to restore the system, the Servicer will accompany that vendor onto MPSCS's premises as needed.
 - Escalate the incident to the appropriate next level of support upon expiration of defined response times.
 - Notify Service Desk that the incident is resolved.
 - Notify MPSCS of case status as defined by the CSP.
 - Provide On-Site Support activity reports to MPSCS if requested.

MPSCS Responsibilities

- Contact Motorola Solutions, as necessary, to request On-Site Support.
- Provide Motorola Solutions with the following pre-defined MPSCS information and preferences for inclusion in the CSP.
 - Case notification preferences and procedure.
 - Repair verification preference and procedure.
 - Escalation procedure forms.
- Submit changes in any information supplied in the CSP to the Service Delivery Manager (SDM).
- Allow servicers access to facilities and equipment.



- Verify with the Service Desk that restoration is complete or system is functional, if required by repair verification preference provided by the MPSCS.
- Cooperate with Motorola Solutions and perform all acts that are reasonable or necessary to enable Motorola Solutions to provide these Fulfillment Services.

(This space is intentionally blank)



SECTION 5

ASTRO 25 CONNECTIVITY SERVICES

5.1 OVERVIEW

Motorola Solutions' ASTRO® 25 Connectivity Service provides network backhaul to support the MPSCS' mission-critical ASTRO 25 communications. The backhaul connection will link the ASTRO 25 core site at 1102 with the Motorola Solutions hosted Data Centers to support the Critical Connect feature. The ASTRO 25 Connectivity Service removes the complexity of multi-vendor management for the ASTRO 25 radio network and backhaul by establishing a fully-managed end-to-end backhaul service. The connection can be provisioned with additional bandwidth as new features are added.

Motorola Solutions will provide and install equipment to support the backhaul service, as described in Section 5.3.6: ASTRO 25 Connectivity Service Sites and Equipment. In addition to providing the backhaul equipment and services, Motorola Solutions will maintain and manage network availability, as described in this Statement of Work. Services in the SOW are delivered by Motorola Solutions and its partners.

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

5.2 PREREQUISITES

The ASTRO 25 Connectivity Service is integrated with existing ASTRO 25 service packages when proposed to connect ASTRO 25 infrastructure. The ASTRO 25 Connectivity Services will use the existing infrastructure Maintenance and Service package that is currently in place. The ASTRO 25 Connectivity Service to MPSCS' ASTRO 25 infrastructure core will be automatically canceled if MPSCS cancels their ASTRO 25 service package.

The use of the features in the "Critical Connect" application is specifically dependent on the communications from the Motorola ASTRO 25 Wave Radio Gateway software to the Critical Connect software located at the Critical Connect data center. The ASTRO 25 Connectivity Service is only offered and available to ASTRO 25 systems that provide Public Safety Radio Services. The service is designed specifically to enable the use of Motorola Solutions information based applications including Smart Connect, Smart Locate, Critical Connect with Wave Communicator, and other cloud and hosted applications provided by Motorola Solutions. The service is not designed to support non Motorola Solutions ASTRO 25 or Application voice or data.



The ASTRO 25 Connectivity service does not require separate service packages to support cloud-hosted Motorola Solutions software products like Cirrus Central Management. The ASTRO 25 Connectivity Service is available to support cloud-hosted applications purchased from Motorola Solutions by MPSCS.

5.3 PRODUCT AND INSTALLATION

5.3.1 Scope

Motorola Solutions will provide and manage connectivity service between MPSCS' ASTRO 25 core site 1102 as noted in Section 5.3.6: ASTRO 25 Connectivity Service Sites and Equipment.

5.3.2 Motorola Solutions Responsibilities

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

- Provide equipment noted in Section 5.3.6: ASTRO 25 Connectivity Service Sites and Equipment to establish connectivity between MPSCS' network elements and MPSCS 1102 site noted in the same table.
- Install equipment supplied by Motorola Solutions. Installation period can be within 45 business days from the time Motorola Solutions receives and processes the order. A final installation schedule will be reviewed and agreed upon jointly with MPSCS to combine the Critical Connect SOW at the Detailed Design Review.
- When available and approved by MPSCS, Motorola Solutions may use MPSCS-owned or MPSCS-managed resources at no additional cost to Motorola Solutions.
- Cooperate with MPSCS to schedule the implementation of the ASTRO 25 Connectivity Service.
- Coordinate the activities of any Motorola Solutions subcontractors necessary to provide this service.
- Administer safe work procedures for installation.
- Assist MPSCS with operating and using the system during cutover.
- Motorola Solutions may, in our own discretion, choose to modify the backhaul design. These changes will result in equivalent or improved capacity, cost, reliability, or availability.

5.3.3 MPSCS Responsibilities

MPSCS will fulfill the following responsibilities to provide the ASTRO 25 Connectivity Service:

- Ensure that Site 1102 meets space, grounding, power, and connectivity requirements for equipment installation.
- Obtain all licensing, site access, or permitting required for project implementation.



- Provide a dedicated delivery point, such as a warehouse, for receipt, inventory, and storage of equipment prior to delivery to the site(s) if requested by Motorola Solutions.
- Ensure existing sites or equipment locations have sufficient space available for the system, as specified by Motorola Solutions' R56 Standards and Guidelines for Communication.
- Ensure that existing sites or equipment locations have adequate electrical power in the proper phase, in the proper voltage, and with necessary site grounding to support the requirements of the equipment provided with the ASTRO 25 Connectivity Service.
- Perform any location upgrades or modifications.
- Obtain and maintain approved local, State, or Federal permits necessary for installing and operating the proposed equipment.
- Provide any required system interconnections not specifically included in the ASTRO 25 Connectivity Service. Links provided by the ASTRO 25 Connectivity Service are outlined in Section 5.3.6: ASTRO 25 Connectivity Service Sites and Equipment.
- Perform work that is necessary to complete the project and is outside the scope of the installation services provided by Motorola Solutions.
- MPSCS shall provide access and accommodations to install wireless LTE back up.
- MPSCS will notify Motorola Solutions of any maintenance that may affect the operating status of the Managed Devices using a Customer Maintenance Change Management Request via the Helpdesk or MyView Portal. Examples of maintenance activities include: powering down the site, a Motorola Solutions' managed device, or a third-party Network Terminating Unit, or resetting, recabling, or moving equipment components.
- If a Motorola Solutions representative visits the MPSCS Site or works remotely, at MPSCS' request, to investigate an issue with the Connectivity services, and the Motorola Solutions representative determines the Connectivity Services are functioning properly or is prevented from resolving the issue because MPSCS did not provide access or reasonable assistance, MPSCS will be charged at published or negotiated time and material rates.
- In the event Motorola Solutions agrees to manage any of MPSCS' equipment components and determines that those components need to be upgraded before Motorola Solutions can manage them, MPSCS will need to perform any upgrades required to support Motorola Solutions' management. Potential upgrades that might be necessary include: upgrades for Managed Device Enhanced Features, end-of-life conditions, and the like. Motorola Solutions will manage those MPSCS equipment components after the necessary upgrade is complete.
- Upon Motorola Solution's request, MPSCS or designated field service technician will reboot the Managed Devices, provide the LED light statuses of the third-party provider Network Terminating Unit where applicable, verify equipment power, verify that cables are securely connected, and insert a loopback plug.



5.3.4 Availability Commitment

Service Level Availability Objectives

Motorola Solutions’ ASTRO 25 Connectivity Service includes service level objectives, calculated using a standard formula. Active network sites during the reporting period will only be monitored for availability when active, so Motorola Solutions will not factor mobile sites not in active use into availability calculations. Motorola Solutions will monitor service availability 24 hours a day, 7 days a week.

Availability Calculation

For the ASTRO 25 Connectivity Service, Motorola Solutions will provide MPSCS with availability metrics for sites. ASTRO 25 Connectivity Service availability is the percentage of time that the circuit is available within a given calendar month.

Motorola Solutions will determine connection availability individually for each of the MPSCS’ ASTRO 25 Connectivity Service connections. Availability is calculated monthly by computing the total number of Critical priority incident outage minutes in a calendar month and dividing that by the total number of minutes in a 30-day calendar month. Availability is calculated after a Critical incident ticket is opened. If the site has backup connectivity, this is factored into the availability calculation. The formula for computing availability is as follows:

$$\text{Availability (\%)} = (1 - (\text{Total minutes of site Hard Outage per month} \div \text{Number of days in month} \times 24 \text{ hours/day} \times 60 \text{ minutes/hour})) \times 100.$$

Table 4-1 provides Motorola Solutions’ availability commitment for the backhaul link. The row below contains the backhaul link specifications including the committed Service Level Agreement, as well as the targeted Service Level Objective.

Table 4-1: ASTRO 25 Connectivity Service Level

Site Type	Link Count	Link Access (Mb)	Handoff (NID to SRX)	Hardware (per link)	Wireless Backup (VRF)	Service Level Agreement	Service Level Objective
ASTRO Core (Primary)	2	100/1000	1000 – LC Fiber	SRX1500	Yes (Critical Connect)	99.5%	100%

Outages

Availability is influenced by multiple factors, including network design, equipment, backhaul, and environmental factors. This section defines outage types, and how they factor into service availability calculations.

Hard Outage

A hard outage, classified as a Priority 1 incident, is a complete loss of Motorola Solutions-provided backhaul connectivity, during which MPSCS cannot use the service and is prepared to release it for immediate testing. Motorola Solutions factors hard outages into availability calculations.

Any delay, act, or omission by MPSCS or a third-party other than a Motorola Solutions-selected local access provider, that causes or extends an outage is



excluded from the availability calculation. In addition, periods of service degradation, such as slow data transmission, where a Priority 1 trouble ticket has not been opened with Verizon and MPSCS has not released its Service for immediate testing

Planned Outages

Planned outages are pauses in service delivery that Motorola Solutions can notify MPSCS of in advance, with a scheduled time for when the outage will end. If a planned outage exceeds the time that was predicted by 10% of the time scheduled, then the outage will be included as an agenda item for discussion at the next meeting between Motorola Solutions and MPSCS. Motorola Solutions and MPSCS will re-categorize the outage during the meeting. Motorola Solutions does not include planned outages in connectivity availability calculations.

Force Majeure

An outage resulting from an incident categorized as *Force Majeure* is not included in availability calculations, but Motorola Solutions will provide continuous commercially reasonable effort to restore system components affected by a *Force Majeure* event.

Availability Exclusions

The following items are excluded from Motorola Solutions’ availability calculations:

- Periods of Soft Outage, during which MPSCS is able to use the ASTRO 25 Connectivity Service, and is not prepared to release the service for immediate testing.
- Sites installed for less than one full calendar month.
- Customer Premises Equipment (“CPE”) not under Motorola Solutions 24/7 monitoring coverage.
- Sites with wireless primary access.
- MPSCS sites with wireless backup access, where wireless signal strength does not meet wireless signal strength guidelines as required by Motorola Solutions.

5.3.5 Service Priority Levels

This section provides descriptions of the Service Priority Levels associated with incident handling and availability measurements.

Table 4-2: ASTRO 25 Connectivity Service Priority Levels

Priority	Criteria	Primary Link Response Times	Secondary Link Response Times
Priority 1 (Critical)	Hard Outage. The ASTRO 25 Connectivity Service is completely inoperable or degraded to the extent that it is unusable by the Customer. The Customer is prepared to release the service for immediate testing.	Monitored 24/7. Response within 15 minutes. Restoration in 3.5 hours.	8x5



Priority	Criteria	Primary Link Response Times	Secondary Link Response Times
Priority 2 (High)	ASTRO 25 Connectivity Service performance is degraded, but the Customer is able to use the Service. Incidents are assigned this priority if the Customer is not prepared to release the service for immediate testing.	Monitored 24/7. Response within 15 minutes. Restoration in 3.5 hours.	8x5
Priority 3 (Medium)	A problem is affecting an ASTRO 25 Connectivity Service component, and that problem does not impact service functionality or availability.	Monitored 24/7. Response within 15 minutes. Restoration in 3.5 hours.	8x5
Priority 4 (Low)	Customer's requests that do not impact the ASTRO 25 Connectivity Service, such as a Customer request for an incident report Service incidents not covered by Critical, High, or Medium priority. Scheduled maintenance.	Monitored 24/7. Response within 15 minutes. Restoration in 3.5 hours.	8x5

5.3.6 ASTRO 25 Connectivity Service Sites and Equipment

Table 4-3 describes sites included in the proposed backhaul design, notes their location, and lists the critical solution equipment provided for them.

Table 4-3: ASTRO 25 Connectivity Service Interconnected Site Locations

Site Name	Site Address	Major Equipment
MPSCS 1102	7200 N. Canal Rd. Dimondale, MI 48917	SRX1500 – Router
MPSCS 1102	7200 N. Canal Rd. Dimondale, MI 48917	AER2200 – Cradlepoint modem
MPSCS 1102	7200 N. Canal Rd. Dimondale, MI 48917	Telco Network Interface Device
MPSCS 1102	7200 N. Canal Rd. Dimondale, MI 48917	Verizon Overture 1400
MPSCS 1102	7200 N. Canal Rd. Dimondale, MI 48917	AT&T Ciena Switch

Motorola will provide, at no charge, local access (provided by Vesta Solutions, a wholly owned subsidiary of Motorola Solutions, Inc.) until September 30, 2022. After that period, local access must be made available by MPSCS for use with ASTRO 25 Connectivity Service. Any subsequent services relying on ASTRO 25 Connectivity Service will not function without local access.



5.4 AVAILABILITY REPORTS

5.4.1 Description of Service

Motorola Solutions will track the availability of MPSCS' ASTRO 25 Connectivity Service components using standardized availability reports, and will take actions to maintain network availability at committed levels based on those reports. Motorola Solutions automatically collects and collates availability data from network elements, and uses that data to determine system health and if any maintenance or improvements are needed. Trend analysis can indicate capacity, availability or reliability issues before they significantly affect services.

5.4.2 Scope

Each month, Motorola Solutions will create and distribute a network availability report to compare with availability levels described in Availability Commitment.

This service includes the following tasks:

- Data Collection—Availability data is remotely collected and stored for reporting purposes.
- Data Reporting—A suite of availability reports is generated and uploaded to MyView Portal.

5.4.3 Inclusions

Availability reports will be provided for Motorola Solutions-provided site connections included as part of the ASTRO 25 Connectivity Service.

5.4.4 Motorola Solutions Responsibilities

- Collect availability data through defined interfaces.
- Provide the availability reports within MyView Portal.
- Provide a Motorola Solutions point of contact to questions MPSCS has about the findings or service reports provided by Motorola Solutions.

5.4.5 Limitations and Exclusions

- Availability degradation is excluded from Motorola Solutions availability target objectives if that degradation results from MPSCS deciding to delay or not take necessary actions. Motorola Solutions will amend availability calculations accordingly.

5.4.6 MPSCS Responsibilities

- Designate an authorized reporting contact to work with Motorola Solutions to address any questions.
- When necessary, perform corrective actions identified by Motorola Solutions' project team as outside the scope of Motorola Solutions' responsibilities.



5.5 BACKHAUL EVENT MONITORING

5.5.1 Description of Service

Backhaul Event Monitoring provides real-time end-to-end event monitoring and fault isolation for ASTRO 25 Connectivity Service backhaul components and links. A set of sophisticated tools support remote detection and classification of events on MPSCS' backhaul network. When an event is detected, Motorola Solutions will determine the status of impacted backhaul links and engage with other service teams as needed to isolate the cause and resolve the incident. Motorola Solutions will respond to incidents based on priority level. Priority and response information is available in Service Priority Levels.

Backhaul Event Monitoring is incorporated into the interface Motorola Solutions' uses for Backhaul Event Monitoring, establishing a single process for MPSCS

5.5.2 Scope

Backhaul Event Monitoring is available 24 hours a day, 7 days a week. Motorola Solutions' tools and processes for monitoring ASTRO 25 radio networks will be leveraged to monitor the backhaul endpoints effectively, and to provide a consistent monitoring experience if receiving both services. Incidents that are generated by the monitoring service will be handled in accordance with the times and priorities as defined in Service Priority Levels.

5.5.3 Inclusions

Backhaul Event Monitoring is provided for the links and equipment listed in ASTRO 25 Connectivity Service Sites and Equipment.

5.5.4 Motorola Solutions Responsibilities

- Use concurrent connectivity through the network connection established to support Backhaul Event Monitoring.
- Verify connectivity and event monitoring after system installation is complete.
- Monitor backhaul links continuously 24 hours per day, 7 days per week.
- Create incident tickets when necessary. Identify and classify the link associated with the incident. Gather information to perform the following:
 - Characterize the issue.
 - Determine a plan of action.
 - Assign and track the incident to resolution.
- Remotely access MPSCS' backhaul to perform remote diagnosis and fault isolation as permitted by MPSCS pursuant to MPSCS Responsibilities.
- Dispatch MPSCS' field service technician designated in the CSP when necessary, and maintain communications with MPSCS until the incident is resolved. Provide updates in accordance with the agreed frequency, until resolution.



5.5.5 Limitations and Exclusions

- Monitoring excludes Customer Enterprise Network (“CEN”) components.
- Additional support charges beyond the contracted service rates may apply if Motorola Solutions determines that system faults were caused by MPSCS making changes to critical system parameters.
- Motorola Solutions is not responsible for system faults or deficiencies that are caused by changes or modifications to the system not performed by Motorola Solutions.

5.5.6 MPSCS Responsibilities

- Provide Motorola Solutions with continuous remote access to enable the monitoring service.
- Provide continuous utility service to any Motorola Solutions backhaul equipment installed or used at the MPSCS’ premises to support delivery of the service. MPSCS agrees to take reasonable due care to secure the Motorola Solutions equipment from theft or damage while on MPSCS’ 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 changes in any information supplied to Motorola Solutions and included in the CSP to the Customer Support Manager (“CSM”).
- Notify the CMSO when MPSCS performs any activity that impacts the backhaul components. Activity that impacts the backhaul components 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.
- Allow Motorola Solutions’ field service technician, 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, designated in the CSP, access to remove Motorola Solutions-owned monitoring equipment upon cancellation of service.
- Provide Motorola Solutions with all MPSCS-managed passwords required to access the MPSCS’ 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 backhaul faults were caused by the MPSCS making changes to critical system parameters without written agreement from Motorola Solutions.
- Cooperate with Motorola Solutions and perform reasonable or necessary acts to enable Motorola Solutions to provide these services.
- Acknowledge that incidents will be handled in accordance with the times and priorities as defined in Service Priority Levels.



5.6 REMOTE TECHNICAL SUPPORT

5.6.1 Description of Service

Motorola Solutions' Remote Technical Support service provides telephone consultation for technical issues that require ASTRO 25 Connectivity Service backhaul knowledge and troubleshooting capabilities. As with ASTRO 25 incidents, the CMSO Service Desk will respond to ASTRO 25 Connectivity Service incidents.

5.6.2 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 the assigned priority. ASTRO 25 Connectivity Service priority levels are defined in Service Priority Levels. Any unresolved incidents will be escalated to Motorola Solutions engineering and Original Equipment Manufacturers ("OEM") for further assistance.

5.6.3 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 MPSCS requests for support.
- Respond to requests for service in accordance with incident priority levels defined in Service Priority Levels.
- Provide caller a plan of action outlining additional requirements, activities, or information required to achieve restoral/fulfillment.
- Maintain communication with MPSCS 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 MPSCS of an alternative course of action.

5.6.4 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.



5.6.5 MPSCS Responsibilities

- Submit 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 MPSCS’ 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 handled in accordance with the committed response times in Service Priority Levels.
- Cooperate with Motorola Solutions, performing acts that are reasonable or necessary to enable Motorola Solutions to provide Remote Technical Support. These actions include, but are not limited to, providing System IP information, local hardware logs, software versions, and MPSCS change management information.

5.7 ON-SITE RESPONSE

Motorola Solutions’ On-site 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.

5.7.1 Description of Service

The Motorola Solutions CMSO Service Desk will receive the MPSCS’ 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 MPSCS’s location to restore the system based on priority levels defined in Service Priority Levels.

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.

5.7.2 Scope

On-site Response is available as needed to support the availability described in Availability Commitment.



5.7.3 Inclusions

On-site Response is provided for hardware included with ASTRO 25 Connectivity Service.

5.7.4 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 MPSCS information, as needed.
- Motorola Solutions designated field service technician will perform the following on-site:
 - Run diagnostics on the component.
 - Perform physical fault restoration and hardware maintenance to restore component functions.
 - 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 MPSCS' premises.
 - If required by MPSCS' repair verification in the Customer Support Plan ("CSP"), verify with the MPSCS that restoration is complete or system is functional. If verification by MPSCS 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 MPSCS or Motorola Solutions on-site service technician, indicating the incident is resolved.
- Notify MPSCS 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 servicer technician on-site, delayed, or closed.
- Provide incident activity reports to MPSCS, if requested.

5.7.5 MPSCS 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 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 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 MPSCS, 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 to provide On-site Response to MPSCS-provided third-party elements, MPSCS agrees to obtain and provide applicable third-party consents or licenses to enable Motorola Solutions to provide the service.

5.8 SOFTWARE UPDATES

5.8.1 Description of Service

Each quarter, Motorola Solutions will provide relevant Original Equipment Manufacturer (“OEM”) software patches for backhaul equipment included as part of the ASTRO 25 Connectivity Service. These patches will update equipment when required to maintain compatibility with components or will address security vulnerabilities.

5.8.2 Scope

Motorola Solutions will update network components when it determines it is necessary to maintain the ASTRO 25 Connectivity Service, and will provide security updates as needed to address identified security vulnerabilities.

Software Updates follow Motorola Solutions’ defined change management process to avoid potential disruption. Once an OEM software update is available, Motorola Solutions initiates the change process to define the update’s impact and work with MPSCS to schedule its implementation.

5.8.3 Inclusions

Motorola Solutions will provide relevant software patches and updates as provided by OEMs based on a schedule mutually agreed by the parties.



5.8.4 Motorola Solutions Responsibilities

- Provide relevant software and security patches to MPSCS when provided by the OEM.
- Notify MPSCS if an update will require network downtime to implement.
- Work with MPSCS to schedule installation of disruptive software patches.

5.8.5 Limitations and Exclusions

- Motorola Solutions does not provide warranties on software updates. Warranties on software updates, if available, will be provided directly by the OEM.

5.8.6 MPSCS Responsibilities

Work with Motorola Solutions to schedule installation of disruptive software patches.

(This space is intentionally blank)



SECTION 6

EQUIPMENT LIST

MOTOROLA SOLUTIONS-PROVIDED EQUIPMENT

NOMENCLATURE	QTY	DESCRIPTION	UNIT LIST (USD)	DISC PRICE (USD)	EXT DISC PRICE (USD)
SQM01SUM0323	1	ASTRO MASTER SITE	\$0.00	\$0.00	\$0.00
CA03517AB	1	ADD: CORE EXPANSION	\$0.00	\$0.00	\$0.00
CA03586AB*	1	ADD: DYNAMIC TRANSCODING	\$40,000.00	\$30,000.00	\$30,000.00
CA03511AB	1	ADD: HIGH AVAILABILITY DATA	\$98,000.00	\$73,500.00	\$73,500.00
T8639	2	JUNIPER FIREWALL APPLIANCE	\$3,200.00	\$2,400.00	\$4,800.00
CLN1868	4	2930F 24-PORT SWITCH	\$2,500.00	\$1,875.00	\$7,500.00
CLN1866	4	FRU: 1M DAC CABLE	\$200.00	\$150.00	\$600.00
SQM01SUM0273A	1	MASTER SITE CONFIGURATION	\$0.00	\$0.00	\$0.00
CA03713AA	2	ADD: CRITICAL CONNECT LMP	\$8,000.00	\$6,000.00	\$12,000.00
CA02629AB	1	ADD: EXPAND 7.16 M CORE	\$0.00	\$0.00	\$0.00
SQM01SUM0284C	2	WAVE RADIO GATEWAY SERVER HARDWARE	\$15,000.00	\$11,250.00	\$22,500.00
SQM01SUM0292A	4	CRYPTPR	\$1,875.00	\$1,406.25	\$5,625.00
CA02066AA	4	ADD: AC LINE CORD, NORTH AMERICA	\$0.00	\$0.00	\$0.00
CA02954AA	4	ADD: SECURE OPERATION	\$3,250.00	\$2,437.50	\$9,750.00
CA02933AA	4	ADD: ASTRO AES 256, DES-OFB, ADP ENCRYPTION KIT	\$1,800.00	\$1,350.00	\$5,400.00
DLN8009	1	FRE: DL380 G10 HC 128GH DAS4X1	\$28,000.00	\$21,000.00	\$21,000.00
MOTOROLA SOLUTIONS-PROVIDED EQUIPMENT TOTAL				EXT LIST TOTAL	EXT DISC TOTAL
				\$256,900	\$192,675

*The Dynamic Transcoding line item above provides qty 2 Core Servers (VMS07 & VMS08). The servers can be used to expand the call capacity of the Critical Connect solution when needed and support Dynamic Transcoding in Zone 1 for TDMA operation.

*HA line item (redundancy option) - includes the redundant CEN LAN switch, RNI-DMZ switch and firewall, PDG, GGSN.



MOTOROLA SOLUTIONS DROPSHIP EQUIPMENT

DESCRIPTION	UNIT LIST	EXT DISC PRICE (USD)
PDU, 5A BREAKERS, 10A BREAKERS	\$3,174	\$2,856

SECTION 7

PROFESSIONAL SERVICES

Motorola Solutions has proposed professional services that include, but are not limited to, the following:

Project Management	
Assign resources, create and maintain project workbook, schedule project kickoff meeting, record and distribute project status meeting minutes, unified communications, complete assigned project tasks according to the project schedule, manufacture Motorola Solutions and non-Motorola Solutions equipment necessary for system based on equipment order, submit project milestone completion documents, obtain TGs, Users, Portal Admin users, execute final project acceptance, transition to service, travel and expenses	\$73,236

Engineer & System Technologist	
Project Administration, review and present the system design and operational requirements for the solution, unified communications, present equipment layout plans and system design drawings, create equipment order and reconcile to contract, verify VMS for LMP installed, verify internetworking firewall, design network plan, remove existing demo WRG and Cryptr and relocate to the Lab, assist with WRG physical install, provide the R56 requirements for space, power, grounding, and connectivity requirements, perform preliminary audit of installed equipment to ensure compliance with requirements and R56 standards, load key to cryptr, note any required changes for inclusion in the "as-built" system documentation, perform functionality test, perform ATP, cutover punchlist, final documentation, travel and expenses	\$120,645

Motorola Services	
Warranty wrap, onsite, equipment freight, and redundant WRG services	\$70,651



SECTION 8

TRAINING

Motorola Solutions will have a webinar for training on how to navigate the Critical Connect portal and Broadband portal as part of the onboarding process. Free courses on LXP (outlined below) for the Critical Connect portal.

Training	Course Number	Hyperlink
Critical Connect		
Critical Connect Portal Training	PSA0032	https://learning.motorolasolutions.com/online/59957enus
WAVE		
WAVE App Overview	PSA0004	https://learning.motorolasolutions.com/search?t=psa0004
WAVE Dispatch Overview	PSA0017	https://learning.motorolasolutions.com/search?t=psa0017
WAVE Interoperability to MOTOTRBO	PSA1051	https://learning.motorolasolutions.com/search?t=psa1051
WAVE Administrator	PSA2001	https://learning.motorolasolutions.com/search?t=psa2001

(This space is intentionally blank)



SECTION 9

BACKHAUL AS SERVICE WITH CRITICAL CONNECT

9.1 MPSCS ENTERPRISE OPTIONS (REQUIRED)

9.1.1 Initial Setup/One time Costs (*Totals from Sections 6 & 7)

Up Front/One Time Costs for Any Options	
Equipment	\$195,532
Professional Services	\$264,531
TOTAL:	\$460,063

*****Initial Setup/One Time Costs will be invoiced to MPSCS upfront within 30 days of receiving a Delivery Order or Notice to Proceed (NTP).**

9.1.2 Single Link (with Wireless Backup)

SINGLE Link Service w/Critical Connect	
\$12,695/month	<ul style="list-style-type: none"> - ASTRO 25 Connectivity Managed Service with 100 Mbps local access (\$4,775).* - Critical Connect ENTERPRISE: (\$5,000). - Simultaneous Talk Paths- 10 (\$200/ea). - API Data Messaging – (\$200/100 subscribers). - Wave Subscribers: 50 (\$13/ea). - Wave Dispatch: 1 (\$70) .

* Motorola will provide, at no charge, local access (provided by Vesta Solutions, a wholly owned subsidiary of Motorola Solutions, Inc.) until September 30, 2022. After that period, local access must be made available by MPSCS for use with ASTRO 25 Connectivity Service. Any subsequent services relying on ASTRO 25 Connectivity Service will not function without local access.



9.2 AVAILABLE FOR PURCHASE TO STATEWIDE AGENCIES AND END USERS:

Critical Connect Options	
\$200/month	One (1) Talk Path for Critical Connect
<p>Each Talk Path accommodates one active voice transmission independent of the number of Talkgroups used. Additional Talk Paths may be purchased from Motorola Solutions by the State of Michigan, Municipalities, or Broadband Push-to-Talk providers to increase the number of simultaneous active voice transmissions.</p>	
\$200/month/100 subscribers	Data API - MESSAGING
\$200/month/100 subscribers	Data API - LOCATION

WAVE Subscribers/Dispatch:	
\$650/month	(50) Wave PTX Safeguard Mobile Subscriptions
\$70/month	Wave PTX Safeguard Web based console



9.3 SUMMARY

9.3.1 Annual Cost

Single Link: ASTRO 25 Connectivity Managed Service with 100Mbps local access and wireless backup*	One-Time Costs	Oct '21 Sep '22	Oct '22 Sep '23	Oct '23 Sep '24	Oct '24 Sept '25	Oct '25 Sept '26	Oct '26 Sept '27	Oct '27 Sept '28	Oct '28 Sept '29	TOTAL
10 Talkpaths										
100 Messaging Subscribers										
50 Wave Subscribers										
1 Wave Dispatch	\$460,063	\$152,340	\$187,936	\$189,004	\$191,237	\$192,404	\$192,368	\$193,606	\$194,843	\$1,953,801
One Time Costs: Equipment/Prof Services										

* Motorola will provide, at no charge, local access (provided by Vesta Solutions, a wholly owned subsidiary of Motorola Solutions, Inc.) until September 30, 2022. After that period, local access must be made available by MPSCS for use with ASTRO 25 Connectivity Service. Any subsequent services relying on ASTRO 25 Connectivity Service will not function without local access.

Michigan's Public Safety Communication System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary System Products

SCHEDULE B- PRICING
MAINTENANCE AND SUPPORT PRICING

	Component	October 1, 2019	October 1, 2020	October 1, 2021	October 1, 2022	October 1, 2023	October 1, 2024	October 1, 2025	October 1, 2026	October 1, 2027	October 1, 2028	TOTAL
MPSCS ASTRO LIFECYCLE	System Upgrade Agreement II (SUAll)	\$4,666,781.89	\$5,119,186.80	\$5,570,726.31	\$5,900,187.68	\$6,460,906.70	\$6,502,411.06	\$6,545,043.90	\$6,589,066.01	\$6,634,415.11	\$6,681,002.78	\$60,669,728.24
	Security Update Services (SUS)	\$100,785.87	\$103,809.45	\$106,923.73	\$118,189.84	\$121,735.54	\$125,387.60	\$135,019.65	\$139,070.24	\$143,242.35	\$147,539.62	\$1,241,703.89
	Technical Support (TS)	\$252,878.41	\$260,464.76	\$268,278.70	\$296,546.12	\$305,442.50	\$314,605.77	\$338,773.22	\$348,936.41	\$359,404.51	\$370,186.64	\$3,115,517.03
	OPSOC	\$34,839.75	\$35,884.94	\$36,961.49	\$40,855.97	\$42,081.65	\$43,344.10	\$46,673.71	\$48,073.92	\$49,516.14	\$51,001.63	\$429,233.31
	Business Relationship Manager	\$260,000.00	\$267,800.00	\$275,834.00	\$284,109.02	\$292,632.29	\$301,411.26	\$310,453.60	\$319,767.21	\$329,360.22	\$339,241.03	\$2,980,608.62
	TOTAL	\$5,315,285.92	\$5,787,145.95	\$6,258,724.23	\$6,639,888.63	\$7,222,798.68	\$7,287,159.79	\$7,375,964.08	\$7,444,913.79	\$7,515,938.33	\$7,588,971.70	\$7,588,971.70
	True Up 10-01-21 to 09-30-29 integrations			\$78,584.00	\$468,079.00	\$686,603.00	\$705,746.00	\$725,536.00	\$745,917.00	\$766,904.00	\$788,518.00	\$4,965,887.00
Critical Connect	Critical Connect			\$95,040.00	\$95,040.00	\$95,040.00	\$95,040.00	\$95,040.00	\$95,040.00	\$95,040.00	\$95,040.00	\$760,320.00
	Astro Connectivity Managed Service			\$57,300.00	\$57,300.00	\$57,300.00	\$57,300.00	\$57,300.00	\$57,300.00	\$57,300.00	\$57,300.00	\$458,400.00
	System Upgrade Agreement II (SUAll)				\$35,596.00	\$36,664.00	\$37,764.00	\$38,897.00	\$40,064.00	\$41,266.00	\$42,503.00	\$272,754.00
	Security Update Services (SUS)				INCLUDED	INCLUDED	INCLUDED	INCLUDED	INCLUDED	INCLUDED	INCLUDED	INCLUDED
	TOTAL	\$0.00	\$0.00	\$230,924.00	\$656,015.00	\$875,607.00	\$895,850.00	\$916,773.00	\$938,321.00	\$960,510.00	\$983,361.00	\$6,457,361.00
MPSCS PREMIER **	PremierOne CAD		\$106,678.14	\$109,878.36	\$119,812.29	\$123,406.92	\$127,108.85	\$135,644.68	\$139,714.22	\$143,905.79	\$148,222.50	\$1,154,371.75
	PremierMDC	\$162,778.86	\$150,358.48	\$154,869.30	\$171,187.28	\$176,322.96	\$181,612.64	\$195,563.48	\$201,430.32	\$207,472.88	\$213,696.68	\$1,815,292.88
	Upgrade - Hardware / Software / Services		\$142,848.92	\$142,848.92	\$153,301.28	\$153,301.28	\$153,301.28	\$160,269.52	\$160,269.52	\$160,269.52	\$160,269.52	\$1,386,679.76
	TOTAL	\$162,778.86	\$399,885.54	\$407,596.58	\$444,300.85	\$453,031.16	\$462,022.77	\$491,477.68	\$501,414.06	\$511,648.19	\$522,188.70	\$4,356,344.39
MPSCS Lab	Lab as a Service (5 Year Agreement)		\$655,000.00	\$674,650.00	\$694,890.00	\$715,736.00	\$737,208.00					\$3,477,484.00
	GRAND TOTAL	\$5,478,064.78	\$6,842,031.49	\$7,419,554.81	\$8,247,158.48	\$9,078,168.84	\$9,192,136.56	\$8,592,977.76	\$8,692,244.85	\$8,794,490.52	\$8,899,678.40	\$81,236,506.48



Schedule H

Subscription Services Schedule

This Subscription Services Schedule (this “**SSS**”) is governed by the State of Michigan Contract No. 190000001544 dated October 1, 2019, as amended (“**Primary Agreement**”), entered into between Motorola Solutions, Inc. and the State of Michigan (“**Customer**”). Capitalized terms used in this SSS, but not defined herein, will have the meanings set forth in the Primary Agreement.

1. Subscription Services.

1.1. Scope. This SSS governs Customer’s purchase of Subscription Services (and, if set forth in an Authorizing Document, as defined in Section 5.1 of Schedule A of the Primary Agreement, related services) from Motorola and provides additional and/or different terms and conditions that govern the sale of Subscription Services. This SSS will be subject to, and governed by, the terms of the Primary Agreement. To the extent there is a conflict or inconsistency between the terms and conditions of the SSS and an associated Authorizing Document, the terms and conditions of the Authorizing Document will take precedence over the SSS. Additional Subscription Services-specific Addenda or other terms and conditions may apply to certain Subscription Services, where such terms are provided or presented to Customer.

1.2. Definitions. Capitalized terms used in this SSS shall have the following meanings:

1.2.1. “Authorized Users” shall mean persons authorized by the Customer to access and use the subscription services, subject to the maximum number of users specified in the applicable Statement of Work.

1.2.2. “Customer Contact Data” shall mean data Motorola collects from Customer, its Authorized Users, and their end users for business contact purposes.

1.2.3. “Customer Data” shall mean data, information, and content, including images, text, videos, documents, audio, telemetry and structured data base records, provided by, through, or on behalf of Customer, its Authorized Users, and their end users through the use of the Subscription Services. Customer Data does not include Customer Contact Data, Service Use Data, or information from publicly available sources or other Third-Party Data or Contractor Data;

1.2.4. “Customer-Provided Equipment” shall mean certain components, including equipment and software, not provided by Motorola that may be required for use of the Subscription Services.

1.2.5. “Motorola-Provided Equipment” shall mean hardware provided by Motorola and not purchased by Customer under this SSS.

1.2.6. “Feedback” shall mean comments or information, in oral or written form, given to Motorola by Customer or Authorized Users, including their end users, in connection with or relating to the Subscription Services, products or services.

1.2.7. “Contractor Data” shall mean data owned or licensed by Motorola;

1.2.8. “Authorizing Documents” shall have the meaning set forth in the Primary Agreement, Schedule A.



- 1.2.9. “Process” or “Processing”** shall mean 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.
- 1.2.10. “Service Use Data”** shall mean data generated by Customer’s use of the Subscription Services or by Motorola’s support of the Subscription Services, including personal information, location, monitoring and recording activity, product performance and error information, activity logs and date and time of use;
- 1.2.11. “Subscription Services”** shall mean hosted software-as-a-service provided to Customer, and other software which is either preinstalled on Motorola-Provided Equipment or installed on Customer-Provided Equipment and licensed to Customer by Motorola on a subscription basis.
- 1.2.12. “Subscription Software”** shall mean software which is either preinstalled on Motorola-Provided Equipment or installed on Customer-Provided Equipment and licensed to Customer by Motorola on a subscription basis associated with the Subscription Services.
- 1.2.13. “Third-Party Data”** shall mean information obtained by Motorola from publicly available sources or its third party content providers and made available to Customer through the Subscription Services.

2. Delivery of Subscription Services.

2.1. Delivery. During the applicable Subscription Term (as defined below), Motorola will provide to Customer the Subscription Services set forth in an Authorizing Document, in accordance with the terms of this SSS. Motorola will provide Customer advance notice (which may be provided electronically) of any planned downtime. Delivery will occur upon Customer’s receipt of credentials required for access to the Subscription Services or upon Motorola otherwise providing access to the Subscription Services. If agreed upon in an Authorizing Document, Motorola will also provide Services related to such Subscription Services.

2.2. Modifications. Motorola may modify the Subscription Services, any associated recurring Services and any related systems so long as their functionality (as described in the applicable Authorizing Document) is not materially degraded. Documentation for the Subscription Services may be updated to reflect such modifications. For clarity, new features or enhancements that are added to any Subscription Services may be subject to additional Fees.

2.3. User Credentials. If applicable, Motorola will provide Customer with administrative user credentials for the Subscription Services, and Customer will ensure such administrative user credentials are accessed and used only by Customer’s employees with training on their proper use. Customer will protect, and will cause its Authorized Users to protect, the confidentiality and security of all user credentials, including any administrative user credentials, and maintain user credential validity, including by updating passwords. Customer will be liable for any use of the Subscription Services through such user credential (including through any administrative user credentials), including any changes made to the Subscription Services or issues or user impact arising therefrom. To the extent Motorola provides Services to Customer in order to help resolve issues resulting from changes made to the Subscription Services through user credentials, including through any administrative user credentials, or issues otherwise created by Authorized Users, such Services will be billed to Customer on a time and materials basis, and Customer will pay all invoices in accordance with the payment terms provided under the Primary Agreement.

2.4. Beta Services. If Motorola makes any beta version of a software application (“**Beta Service**”)



available to Customer, Customer may choose to use such Beta Service at its own discretion, provided, however, that Customer will use the Beta Service solely for purposes of Customer's evaluation of such Beta Service, and for no other purpose. Customer acknowledges and agrees that all Beta Services are offered "as-is" and without any representations or warranties or other commitments or protections from Motorola. Motorola will determine the duration of the evaluation period for any Beta Service, in its sole discretion, and Motorola may discontinue any Beta Service at any time. Customer acknowledges that Beta Services, by their nature, have not been fully tested and may contain defects or deficiencies.

2.5. Motorola-Provided Equipment Title. Unless Customer is purchasing Equipment pursuant to the terms in the Primary Agreement and unless stated differently in this SSS or in the Authorizing Documents, title to any Motorola-Provided Equipment provided to Customer in connection with the Subscription Services remains vested in Motorola at all times. Any sale of Equipment pursuant to this SSS will be governed by the terms and conditions set forth in the Primary Agreement.

3. Subscription Software License, Restrictions, and Obligations.

3.1. Subscription Software License. Subject to Customer's and its Authorized Users' compliance with this SSS, including payment terms, Motorola hereby grants Customer and its Authorized Users a limited, non-transferable, non-sublicenseable, and non-exclusive license to use the Subscription Software identified in an Authorizing Document, and the associated Documentation, solely for Customer's internal business purposes. The foregoing license grant will be limited to use in the territory and to the number of licenses set forth in an Authorizing Document (if applicable), and will continue for the applicable Subscription Term. Customer may access, and use the Subscription Software only in Customer's owned or controlled facilities, including any authorized mobile sites; provided, however, that Authorized Users using authorized mobile or handheld devices may also log into and access the Subscription Services remotely from any location. No custom development work will be performed under this Addendum.

3.2 End User Licenses. Notwithstanding any provision to the contrary in this SSS, certain Subscription Software is governed by a separate license, EULA, or other agreement, including terms governing third-party software, such as open source software, included in the Subscription Software. Except to the extent prohibited by law, Customer and its Authorized Users will comply with such additional license agreements. Prior to the use of a particular Subscription Service, Customer has the right to review additional license agreements applicable to Subscription Software. Motorola will use commercially reasonable efforts to: (i) determine whether any open source or third-party licensed software is provided under a Subscription Service; (ii) identify the open source or third-party licensed software and provide Customer a copy of the applicable open source or third-party software license (or specify where that license may be found); and, (iii) provide Customer a copy of the open source software source code, without charge, if it is publicly available.

3.3 Customer Restrictions. Customers and Authorized Users will comply with the applicable Documentation and the copyright laws of the United States and all other relevant jurisdictions in connection with their use of the Subscription Services. Customer will not, and will not allow others including the Authorized Users, to make the Subscription Software and Subscription Services available for use by unauthorized third parties, including via a commercial rental or sharing arrangement; reverse engineer, disassemble, or reprogram software used to provide the Subscription Software or Subscription Services or any portion thereof to a human-readable form; modify, create derivative works of, or merge the Subscription Software or software used to provide the Subscription Software or Subscription Services with other software; copy, reproduce, distribute, lend, or lease the Subscription Software, Subscription Services or Documentation for or to any third party; take any action that would cause the Subscription Software, software used to provide the Subscription Services, or Documentation to be placed in the public domain; use the Subscription Software or Subscription Services to compete with Motorola; remove, alter, or obscure, any copyright or other notice; share user credentials (including among Authorized Users); use the



Subscription Software or Subscription Services to store or transmit malicious code; or attempt to gain unauthorized access to the Subscription Software, Subscription Services or its related systems or networks.

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

3.5 Non-Motorola Content. In certain instances, Customer may be permitted to access, use, or integrate Customer or third-party software, services, content, and data that is not provided by Motorola (collectively, "Non-Motorola Content") with or through the Subscription Services. If Customer accesses, uses, or integrates any Non-Motorola Content with the Subscription Services, Customer will first obtain all necessary rights and licenses to permit Customer's and its Authorized Users' use of the Non-Motorola Content in connection with the Subscription Services. Customer will also obtain the necessary rights for Motorola to use such Non-Motorola Content in connection with providing the Subscription Services, including the right for Motorola to access, store, and process such Non-Motorola Content, and to otherwise enable interoperation with the Subscription Services. Customer represents and warrants that it will obtain the foregoing rights and licenses prior to accessing, using, or integrating the applicable Non-Motorola Content with the Subscription Services, and that Customer and its Authorized Users will comply with any terms and conditions applicable to such Non-Motorola Content. If any Non-Motorola Content require access to Customer Data (as defined below), Customer hereby authorizes Motorola to allow the provider of such Non-Motorola Content to access Customer Data, in connection with the interoperation of such Non-Motorola Content with the Subscription Services. Customer acknowledges and agrees that Motorola is not responsible for, and makes no representations or warranties with respect to, the Non-Motorola Content (including any disclosure, modification, or deletion of Customer Data resulting from use of Non-Motorola Content or failure to properly interoperate with the Subscription Services). If Customer receives notice that any Non-Motorola Content must be removed, modified, or disabled within the Subscription Services, Customer will promptly do so. Motorola will have the right to disable or remove Non-Motorola Content if Motorola believes a violation of law, third-party rights, or Motorola's policies is likely to occur, or if such Non-Motorola Content poses or may pose a security or other risk or adverse impact to the Subscription Services, Motorola, Motorola's systems, or any third party (including other Motorola customers). Nothing in this Section will limit the exclusions set forth in Section 33 – Infringement, Indemnification and Remedies of the Primary Agreement.



4 Term.

4.1 Subscription Terms. The duration of Customer's subscription to the Subscription Services and any associated recurring Services ordered under this SSS (or the first Subscription Services or recurring Service, if multiple are ordered at once) will commence upon delivery of such Subscription Services (and recurring Services, if applicable) and will continue for a twelve (12) month period or such longer period identified in an Authorizing Document (the "**Initial Subscription Period**"). Following the Initial Subscription Period, Customer's subscription to the Subscription Services and any recurring Services will automatically renew for additional twelve (12) month periods or longer if agreed to by the parties (each, a "**Renewal Subscription Year**"), unless either Party notifies the other Party of its intent not to renew at least thirty (60) days before the conclusion of the then-current Subscription Term. (The Initial Subscription Period and each Renewal Subscription Year will each be referred to herein as a "**Subscription Term**".) Motorola may increase Fees prior to any Renewal Subscription Year. In such case, Motorola will notify Customer of such proposed increase no later than thirty (30) days prior to commencement of such Renewal Subscription Year. Unless otherwise specified in the applicable Authorizing Document, if Customer orders any additional or subsequent Subscription Services or recurring Services under this SSS during an in-process Subscription Term, the subscription for each such additional or subsequent Subscription Services or recurring Service will (a) commence upon delivery of such Subscription Services or recurring Service, and continue until the conclusion of Customer's then-current Subscription Term (a "**Partial Subscription Year**"), and (b) automatically renew for Renewal Subscription Years thereafter, unless either Party notifies the other Party of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. Thus, unless otherwise specified in the applicable Authorizing Document, the Subscription Terms for all Subscription Services and recurring Services hereunder will be synchronized.

4.2 Term. The term of this SSS (the "**SSS Term**") will commence upon the effective date of the Contract Change Notice, and will continue until the expiration or termination of all Subscription Terms under this SSS, unless this SSS or the Primary Agreement is earlier terminated in accordance with the terms of the Primary Agreement.

4.3 Termination. Notwithstanding the termination provisions of the Primary Agreement, Motorola may terminate this SSS (or any Addendum or Authorizing Document hereunder), or suspend delivery of Subscription Services or Services, upon 30 days' notice to Customer if Customer breaches **Section 3 – Subscription Software License and Restrictions** of this SSS, or any other provision related to Subscription Services terms of service, Subscription Software license scope, or other terms set forth in an Addendum or Authorizing Document, and fails to remedy or cure the breach within the 30 day notice period. Notwithstanding the termination provision in this Schedule or of the Primary Agreement, Motorola may suspend delivery of Subscription Services if it determines that Customer's use of the Subscription Services poses, or may pose, a security or other risk or adverse impact to any Subscription Services, Motorola, Motorola's systems, or any third party (including other Motorola customers). Customer acknowledges that Motorola may have made a considerable investment of resources in the development, marketing, and distribution of the Subscription Services and Documentation, and that Customer's breach of this SSS may result in irreparable harm to Motorola for which monetary damages may be inadequate. If Customer breaches this SSS, in addition to termination, Motorola will be entitled to seek all available remedies at law or in equity (including immediate injunctive relief).

4.4 Return of Discount. If Customer is afforded a discount in exchange for a term commitment longer than one-year, early termination by Customer will result in an early termination fee,



representing a return of the discount off of list price.

4.5 Credits. If a subscription is terminated for any reason prior to the end of the Subscription Term and Customer has prepaid said subscription, Motorola agrees the Customer may be entitled to a credit equal to the amount of the subscription paid in advance but not yet used or consumed.

4.6 The following shall apply to the Subscription Service for Critical Connect, if applicable:

4.6.1 Service Tiers. The Customer can upgrade the service to higher tiers or downgrade to a lower tier. Additionally, the Customer can stack multiple tiers together (additional setup fees may be required if upgrading to higher capacity levels). When the Customer performs a tier upgrade or downgrade, the service term will be reset and a new three (3) year Critical Connect Term will commence.

4.6.2 Port Restrictions. The Motorola on-premise gateway utilizes an ISSI connection and port. This connection is to be used only by the Motorola on-premise gateway in accordance with this service. Use of this ISSI connection and port with any other non-approved gateway is strictly prohibited.

4.7 Suspension of Services. Motorola may terminate or suspend any Subscription Services or Services under an Authorizing Document if Motorola determines: (a) the related Subscription Software license has expired or has terminated for any reason; (b) the applicable Subscription Services is being used on a Customer provided hardware platform, operating system, or version that is not approved by Motorola; (c) Customer fails to make any payments when due.

4.8 Wind Down of Subscription Services. In addition to the termination rights in the Primary Agreement, Motorola may terminate any Authorizing Document and Subscription Term, in whole or in part, in the event Motorola plans to cease offering the applicable Subscription Services to customers upon sixty (60) days' notice unless otherwise stated in the applicable SOW.

4.9 Wind Effect of Termination or Expiration. Upon termination for any reason or expiration of the Primary Agreement, this SSS, an Addendum, or an Authorizing Document, Customer and the Authorized Users will return or destroy (at Motorola's option) all Motorola Materials and Motorola's Confidential Information in their possession or control and, as applicable, provide proof of such destruction. If Customer has any outstanding payment obligations under this SSS, such payment obligations will be paid by Customer in accordance with the Primary Agreement. Notwithstanding the reason for termination or expiration, Customer must pay Motorola for Subscription Services already delivered.

5 Payment.

5.1 Payment. Unless otherwise provided in an Authorizing Document (and notwithstanding the provisions of the Primary Agreement), Customer will prepay an annual subscription Fee set forth in an Authorizing Document for each Subscription Services and associated recurring Service, before the commencement of each Subscription Term. For any Partial Subscription Year, the applicable annual subscription Fee will be prorated based on the number of months in the Partial Subscription Year. The annual subscription Fee for Subscription Services and associated recurring Services may include certain one-time Fees, such as start-up fees, license fees, or other fees set forth in an Authorizing Document.

5.2 No Price Guarantee. Notwithstanding any language to the contrary, the pricing and Fees



associated with this SSS will not be subject to any most favored pricing commitment or other similar low price guarantees.

5.3 Taxes. The Fees do not include any excise, sales, lease, use, property, or other taxes, assessments, duties, or regulatory charges or contribution requirements (collectively, "Taxes"), all of which will be paid by Customer, except as exempt by law, unless otherwise specified in an Authorizing Document. If Motorola is required to pay any Taxes, Customer will reimburse Motorola for such Taxes (including any interest and penalties) within thirty (30) days after Customer's receipt of an invoice, unless Customer furnishes Motorola applicable tax-exemption certificates. Customer will be solely responsible for reporting the Subscription Services for personal property tax purposes, and Motorola will be solely responsible for reporting taxes on its income and net worth.

5.4 Invoicing. The invoicing and payment terms under the Primary Agreement apply.

5.5 License True-Up. Annually, Motorola will have the right to conduct an audit of total user licenses credentialed by Customer for any Subscription Services during a Subscription Term, and Customer will cooperate with such audit. If Motorola determines that Customer's usage of the Subscription Services during the applicable Subscription Term exceeded the total number of licenses purchased by Customer, Motorola may invoice Customer for the additional licenses used by Customer, pro-rated for each additional license from the date such license was activated, and Customer will pay such invoice in accordance with the payment terms in the Primary Agreement.

6 Liability.

6.1 ADDITIONAL EXCLUSIONS. SUBSCRIPTION SERVICES ARE NOT COVERED BY THE WARRANTY PROVISION IN SECTION 23 OF THE PRIMARY AGREEMENT. IN ADDITION TO THE EXCLUSIONS IN SECTIONS 32, 33 AND SECTION 34 LIMITATION OF LIABILITY AND DISCLAIMER OF DAMAGES AS SET FORTH IN THE PRIMARY AGREEMENT, AND NOTWITHSTANDING ANY PROVISION OF PRIMARY AGREEMENT TO THE CONTRARY, MOTOROLA WILL HAVE NO LIABILITY FOR (A) INTERRUPTION OR FAILURE OF CONNECTIVITY, VULNERABILITIES, OR SECURITY EVENTS UNLESS CAUSED SOLELY BY MOTOROLA; (B) DISRUPTION OF OR DAMAGE TO CUSTOMER'S OR THIRD PARTIES' SYSTEMS, EQUIPMENT, OR DATA, INCLUDING DENIAL OF ACCESS TO USERS, OR SHUTDOWN OF SYSTEMS CAUSED BY INTRUSION DETECTION SOFTWARE OR HARDWARE; (C) AVAILABILITY OR ACCURACY OF ANY DATA AVAILABLE THROUGH THE SUBSCRIPTION SOFTWARE OR SERVICES, OR CUSTOMER'S INTERPRETATION, USE, OR MISUSE THEREOF; (D) TRACKING AND LOCATION-BASED SERVICES UNLESS DAMAGES ARE CAUSED BY MOTOROLA; (E) BETA SERVICES; (F) CUSTOMER DATA, INCLUDING ITS TRANSMISSION TO MOTOROLA; (G) CUSTOMER-PROVIDED EQUIPMENT, NON-MOTOROLA CONTENT, THE SITES, OR THIRD-PARTY EQUIPMENT, HARDWARE, SOFTWARE, DATA, OR OTHER THIRD-PARTY MATERIALS, OR THE COMBINATION OF SUBSCRIPTION SERVICES WITH ANY OF THE FOREGOING; (H) LOSS OF DATA OR HACKING UNLESS CAUSED SOLELY BY MOTOROLA; (I) MODIFICATION OF SUBSCRIPTION SERVICES BY ANY PERSON OTHER THAN MOTOROLA; (J) RECOMMENDATIONS PROVIDED IN CONNECTION WITH THE SUBSCRIPTION SERVICES; (K) DATA RECOVERY SERVICES OR DATABASE MODIFICATIONS UNLESS CAUSED BY MOTOROLA; OR (L) CUSTOMER'S OR ANY AUTHORIZED USER'S BREACH OF THIS SSS OR MISUSE OF THE SUBSCRIPTION SERVICES.

6.2 Voluntary Remedies. Motorola is not obligated to remedy, repair, replace, or refund the purchase price for the disclaimed or excluded issues in the Primary Agreement or **Section 6.1 – Additional Exclusions** above, but if Motorola agrees to provide Services to help resolve such



issues, Customer will pay Motorola for its reasonable time and expenses, including by paying Motorola any Fees set forth in an Authorizing Document for such Services, if applicable.

7 Proprietary Rights; Data; Feedback.

7.1 Motorola Materials. Customer acknowledges that Motorola may use or provide Customer with access to software, tools, data, and other materials, including designs, utilities, models, methodologies, systems, and specifications, which Motorola has developed or licensed from third parties (including any corrections, bug fixes, enhancements, updates, modifications, adaptations, translations, de-compilations, disassemblies, or derivative works of the foregoing, whether made by Motorola or another party) (collectively, "Motorola Materials"). The Subscription Services, Contractor Data, Third-Party Data, and Documentation, are considered Motorola Materials. Except when Motorola has expressly transferred title or other interest to Customer by way of an Authorizing Document or under the Primary Agreement, the Motorola Materials are the property of Motorola or its licensors, and Motorola or its licensors retain all right, title and interest in and to the Motorola Materials (including, all rights in patents, copyrights, trademarks, trade names, trade secrets, know-how, other intellectual property and proprietary rights, and all associated goodwill and moral rights). For clarity, this SSS does not grant to Customer any shared development rights in or to any Motorola Materials or other intellectual property, and Customer agrees to execute any documents and take any other actions reasonably requested by Motorola to effectuate the foregoing. Motorola and its licensors reserve all rights not expressly granted to Customer, and no rights, other than those expressly granted herein, are granted to Customer by implication, estoppel or otherwise. Customer will not modify, disassemble, reverse engineer, derive source code or create derivative works from, merge with other software, distribute, sublicense, sell, or export the Subscription Services or other Motorola Materials, or permit any third party to do so.

7.2 Ownership of Customer Data. Customer retains all right, title and interest, including intellectual property rights, if any, in and to Customer Data. Motorola acquires no rights to Customer Data except those rights granted under this SSS including the right to Process and use the Customer Data as set forth in Section 7.3 – Processing Customer Data below and in other applicable Addenda. 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 is the processor, and may engage sub-processors pursuant to Section 7.3.3 – Sub-processors.

7.3 Processing Customer Data.

7.3.1 Motorola Use of Customer Data. To the extent permitted by law, Customer grants Motorola 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 (if Motorola provides Customer Data to a third party that is not a Permitted Subcontractor, such Customer Data will be anonymized) to (a) perform Services and provide Subscription Services under this SSS, (b) analyze the Customer Data to operate, maintain, manage, and improve Motorola products and services, and (c) create new products and services from anonymized Customer Data. Customer agrees that this SSS, along with the Documentation, 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 Change Order process. 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.



7.3.2 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 the Subscription Services), and Motorola's use of such Customer Data in accordance with this SSS, will not violate any laws or applicable privacy notices or infringe any third-party rights (including intellectual property and privacy rights). Customer also represents and warrants that the Customer Data will be accurate and complete to the best of its knowledge, and that Customer has obtained all required consents, provided all necessary notices, and met any other applicable legal requirements with respect to collection and use (including Motorola's and its subcontractors' use) of the Customer Data as described in this SSS.

7.3.3 Sub-processors. Customer agrees that Motorola may engage sub-processors who in turn may engage additional sub-processors to Process data in accordance with this SSS. When engaging sub-processors, Motorola will enter into agreements with the sub-processors to bind them to data processing obligations as required by this Schedule and the Primary Agreement or to the extent required by law.

7.4 Data Retention and Deletion. Except for anonymized Customer Data, as described above, or as otherwise provided under this SSS, Motorola will delete all Customer Data following termination or expiration of this SSS, the applicable Addendum, or Authorizing Document, 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 in writing before expiration or termination, subject to Section 17.7 – Notices of the Primary Agreement. Motorola will have no obligation to retain such Customer Data beyond expiration or termination unless the Customer has purchased extended storage from Motorola through a mutually executed Authorizing Document.

7.5 Service Use Data. Customer understands and agrees that Motorola may collect and use Service Use Data for its own purposes, including the uses described below. Motorola may use Service Use Data to (a) operate, maintain, manage, and 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. Only anonymized Service Use Data may be disclosed to third parties that are not Permitted Subcontractors. It is Customer's responsibility to notify Authorized Users of Motorola's 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 that it has complied and will continue to comply with this Section.

7.6 Third-Party Data and Contractor Data. Contractor Data and Third-Party Data may be available to Customer through the Subscription Services. Customer and its Authorized Users may use Contractor Data and Third-Party Data as permitted by Motorola and the applicable Third-Party Data provider, as described in an Authorizing Document or Subscription Services-specific Addendum. Unless expressly permitted in the applicable Addendum, Customer will not, and will ensure its Authorized Users will not: (a) use the Contractor 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. Additional restrictions may be set forth in the applicable Addendum. Any rights granted to Customer or Authorized Users with respect to Contractor Data or Third-Party Data will immediately terminate upon termination or expiration of the applicable Addendum,



Authorizing Document, or this SSS. Further, Motorola or the applicable Third-Party Data provider may suspend, change, or terminate Customer's or any Authorized User's access to Contractor 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 this SSS, applicable law or Motorola's agreement with the applicable Third-Party Data provider. Upon termination of Customer's rights to use any Contractor 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. Notwithstanding any provision of this SSS to the contrary, Motorola will have no liability for Third-Party Data or Contractor Data available through the Subscription Services. Motorola and its Third-Party Data providers reserve all rights in and to Contractor Data and Third-Party Data not expressly granted in an Addendum or Authorizing Document.

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

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

8 Security.

8.1 Industry Standard. Motorola will maintain industry standard security measures to protect the Subscription Services from intrusion, breach, or corruption. During the term of this SSS, if the Subscription Services enables access to Criminal Justice Information ("CJI"), as defined by the Criminal Justice Information Services Security Policy ("CJIS"), Motorola will provide and comply with a CJIS Security Addendum.

8.2 Background checks. Motorola will require its personnel that access CJI to submit to a background check based on submission of FBI fingerprint cards.

8.3 Customer Security Measures. Customer is independently responsible for establishing and maintaining its own policies and procedures and for ensuring compliance with CJIS and other security requirements, that may apply and are outside the scope of the Subscription Services provided. Customer must establish and ensure compliance with access control policies and procedures, including password security measures. Further, Customer must maintain industry standard security measures. Motorola disclaims any responsibility or liability whatsoever for the security or preservation of Customer Data or Customer Contact Data once accessed or viewed by Customer or its representatives. Motorola further disclaims any responsibility or liability whatsoever that relates to or arise from Customer's failure to maintain industry standard security measures and controls, including but not limited to lost or stolen passwords. Motorola reserves the right to terminate the Subscription Services if Customer's failure to maintain or comply with industry standard security and control measures negatively impacts the Subscription Services or Motorola's own security measures.



8.4 Breach Response Plan. Both parties will maintain and follow a breach response plan consistent with the standards of their respective industries.

9 General Provisions.

9.1 Third-Party Beneficiaries. This SSS is entered into solely between, and may be enforced only by, the Parties. Each Party intends that this SSS will not benefit, or create any right or cause of action in or on behalf of, any entity other than the Parties.

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

9.3 Audit; Monitoring. Motorola will have the right to monitor and audit use of the Subscription Services, which may also include access by Motorola to Customer Data and Service Use Data. Customer will provide notice of such monitoring to its Authorized Users and obtain any required consents, including individual end users, and will cooperate with Motorola in any monitoring or audit. Customer will maintain during the Subscription Term, and for two (2) years thereafter, accurate records relating to any Authorized Users under this SSS to verify compliance with this SSS. Motorola or a third party (“Auditor”) may inspect Customer’s and, as applicable, Authorized Users’ premises, books, and records during normal business hours. Motorola will pay expenses and costs of the Auditor, unless Customer is found to be in violation of the terms of this SSS, in which case Customer will be responsible for such expenses and costs not to exceed \$100,000, Customer will have no obligation to pay audit expenses and costs for the License True-Up under Section 5.5 of this SSS.

9.4 Survival. The following provisions will survive the expiration or termination of this SSS for any reason: **Section 4 – Term; Section 5 – Payment; Section 6.1 – Additional Exclusions; Section 7 – Proprietary Rights; Data, Feedback, Section 8 – General Provisions**, and where the context of any section indicates an intent that such section shall survive the term of this SSS, then such section shall survive.



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **1**
 to
 Contract Number **19000001544**

CONTRACTOR	MOTOROLA SOLUTIONS INC
	500 W. Monroe St.
	Chicago, IL 60661
	Melanie Leenhouts
	616-706-1723
	melanie.leenhouts@motorolasolutions.com
	CV0016903

STATE	Program Manager	Kate Jannereth	DTMB
		517-881-1031	
	jannerethk@Michigan.gov		
	Contract Administrator	Valerie Hiltz	DTMB
(517) 249-0459			
hiltzv@michigan.gov			

CONTRACT SUMMARY

MPSCS CONTINUED SYSTEM UPDATES, EQUIPMENT, MAINTENANCE AND UPGRADES, AND ANCILLARY SYSTEMS PRODUCTS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
October 1, 2019	December 31, 2029	0 - 0 Year	December 31, 2029
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45		As per Delivery Order	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input checked="" type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

N/A

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		December 31, 2029
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$99,900,000.00	\$0.00	\$99,900,000.00		

DESCRIPTION

Effective September 25, 2020 this contract is adding Schedule A, Attachment 9 - Astro 25 Lab as a Service (LaaS) solution as attached. Schedule B Pricing is revised as attached. The Contractor's Contract Administrator has been changed to Melanie Leenhouts. All other terms, conditions, specification and pricing remain the same. Per Contractor and Agency agreement and DTMB Central Procurement Services approval.

TABLE OF CONTENTS

Section 1

On Prem ASTRO 25 Lab as a Service Solution (LaaS).....1-1

1.1 Overview1-1

1.2 The Solution1-1

1.2.1 P25 LaaS Solution:.....1-1

1.3 Installation Requirements.....1-5

1.3.1 MPSCS Responsibilities.....1-5

1.4 CommandCentral Aware Product Description.....1-7

1.5 Mapping Description1-8

1.6 Location on PTT Description1-8

1.7 Location on PTT Features.....1-8

1.8 Geographic Information System (GIS) Data Set Integration1-9

Section 2

LaaS Services.....2-1

2.1 Services Overview2-1

2.2 Technical Support2-1

2.3 Security Update Service (SUS).....2-1

2.4 System Upgrade Service (SUAll).....2-2

2.5 Preventive Maintenance.....2-2

2.6 Network Hardware Repair2-3

2.7 Maintenance Onsite Support.....2-3

Section 3

Lab as a Service (LaaS) Technical Resource.....3-1

3.1 Overview3-1

3.1.1 Specific Duties.....3-2

3.1.2 Skills3-2

3.1.3 Education/Experience3-3

Section 4

Proposal Pricing.....4-1

4.1 Proposal Subscription Pricing4-1

SECTION 1

ON PREM ASTRO 25 LAB AS A SERVICE SOLUTION (LAAS)

1.1 OVERVIEW

Public safety agencies and state officials in every city are in constant search for the best and most cost-effective solution to address the complexities involved in protecting and serving their communities. An advanced, secure and reliable communications system is vital to their mission. Lives often depend on calls getting through to the right person at the right time, so that a fast and coordinated response can be put into action.

Land mobile radio (LMR) system management has grown especially complex over the past two decades, as the system becomes more IP-based. LMR systems must seamlessly interact and connect with applications, software and broadband networks—all of which are moving targets. With unprecedented **interoperability**, **cybersecurity** and **performance** requirements, keeping pace with evolving system capabilities and IP-based technology can be a time-consuming and expensive undertaking.

Mitigating SW/HW/Updates compatibility risk is an important part of a system operator's focus, hence verification and validation testing is an important part of maintaining high availability and performance standard of a large complex statewide P25 system as MPSCS. A test lab environment requires investment and maintenance to ensure it is fit for purpose as new SW and HW features are tested.

Fortunately, there is an option.

1.2 THE SOLUTION

Motorola's Managed Services ASTRO 25 Lab as a service (LaaS) is a service that provides an on premise ASTRO 25 M3 core, provided through an annual fee.

This service is aimed at customers that do not want to take on additional complexity and incur the capital costs to purchase and maintain a lab environment. Motorola stands behind the lab core by providing a complete and current solution including all software and hardware upgrades, security updates and service maintenance.

The provisioning, configuration, verification and validation testing of the HW/SW will be the responsibility of the MPSCS operations staff. Motorola will provide a dedicated lab technical resource to support verification and validation activities.

1.2.1 P25 LaaS Solution:

- ASTRO P25 lab, HW/SW of the non-production test core will be aligned with the MPSCS production system
- New features can be installed and tested on-prem in a non-production environment

- An SUAII included as part of the solution will ensure that the SW/HW is upgraded and refreshed to align with the MPSCS production system.
- Technical support from Motorola Solutions
- Security and new systems updates are regularly patched.
- Dedicated LaaS located on premise at MPSCS and available 24X7
- System Technologist dispatched onsite 8X5 business days for maintenance related issues.
- 8x5 business days' local service support for ongoing core maintenance

The on-premise lab is owned and maintained by Motorola Solutions. It enables an “**evergreen**” platform by refreshing network core components to keep the system supported and enhancing the system with new SW features as they become available. (Additional system expansion for SW features or HW not included) Additionally, Motorola Solutions manages critical component health and provides service support and onsite maintenance services.

The Benefits

Customers benefit from a wide range of services:

SERVICE	BENEFIT
ON Premise ASTRO P25 LaaS at the MPSCS Lab facilities	Allows hands on testing by MPSCS network engineers to perform HW/SW verification and validation testing of new features on a non-production system. This will expedite the introduction of new value-added services for MPSCS users.
LaaS system in alignment with the production network	LaaS will remain aligned with the SW release level and active features of the production system
Predictable payment structure that is paid annually.	A predictable annual fee for the test core, frees up capital to be spent on other network expansions.
Embedded Maintenance Services	Motorola Solutions' managed service framework provides system maintenance duties.
Network Security Services	Regularly available software and services to protect and secure the network
Continual Technology Refresh	Motorola Solutions implements planned technology refresh to the ASTRO 25 LaaS solution to keep it current and supported through the embedded SUAII
Tactical Exercises	MPSCS operations team can enable and execute emergency response plans for hurricane exercises and other emergency response events
Staff Training and development	Allows a sandbox environment for training and development of MPSCS operational staff
Onsite Lab Technical Resource	A lab technical resource that will provide day to day support for lab verification and validation activities.

P25 ASTRO LaaS BASE SOLUTION

The LaaS will include qty 2 Virtual Management Servers (VMS)

- 2 Core Lan Switches, 2 Core Edge Routers,
- 2 Core Mediation Switches (Zone core Protection)
- TRAK Timing Server
- One GGSN (for Data)

- Enablement Server
- Syslog Server
- 1 Intrusion Detection Service
- Intelligent Middleware Server (IMW)
- CEN switch and Firewall
- Internetworking Firewall
- Set of HW spares.

The following management application software will be included and supported on the redundant core VMS servers:

- Unified Network Configuration (UNC)
- Security Partitioning
- Provision Manager
- Unified Event Manager (UEM)
- Firewall Manager
- Backup and Recovery (BAR)
- Air Traffic Interface (ATIA)
- Zone Statistics
- Zone Watch
- Email Alerting
- Zone Historical Reports
- Affiliation User Reports
- Radio Control Manager (RCM)

A Network Manager Client Workstation (Z2 Mini) with 19' Monitor is included to support the above management applications. The client may be located in the Test Lab room or in the NCC room.

The LaaS provides:

1.	Current network features as defined below
2.	NEW network features for testing purposes as defined below, for MPSCS consideration

1. The LaaS will include and align to the CURRENT Network features:

- ASTRO FDMA Trunking Operation License
- ASTRO FDMA Site Licenses Qty 3
- MCC7500 Console Operator Licenses Qty 5
- 500 Radio User License
- Classic Data P25 Trunked Site Qty3
- 700/800 Mixed Site Operation

Aligning with the CURRENT network, an Intelligent Middleware (IMW) server is included on the LaaS to enable testing of Data applications and interfaces to desired applications such as GPS Location and Personnel Accountability. The IMW will be equipped with the following licenses

- 100 Presence Licenses
- 100 Location Licenses

The LaaS will include Core Backhaul Switches capable of supporting Ethernet connected RF Sites or Console Sites. Note that RF site(s) and Console sites are not included. Also note that the existing

MCC7500E Operator Position will remain in the Test Lab for use on the LaaS. Licenses to upgrade the existing Operator Position to 160 Radio Resources have been included.

A Firewall and DMZ Switch has also been included to support a CEN to test applications that require interfacing outside the Motorola RNI into the State of MI network.

1. New Solutions included for testing purposes

The LaaS also includes the following NEW network features for MPSCS consideration and testing:

- Phase 2 TDMA Trunking Operation License
- Phase 2 TDMA Trunking Site License (Qty3)
- Phase 2 TDMA Trunking Dynamic Talkgroup assignment Site License Qty 3
- Dynamic Transcoder
- Transcoded Simultaneous Calls (Qty 5)
- Trunked Enhanced Data Operation License
- Enhanced Data Trunked Site Qty 3
- 500 Enhanced Trunked Data User Licenses
- MCC7500 Console Group Text Licenses Qty 5
- Group Services (includes the below items)
 - 500 Radio Alias Group Download User Licenses with User Login Alias Update
 - 50 Talkgroup Text Messaging Licenses
 - 10 Console Group Text Licenses
- 500 Location on PTT User Licenses
- Fire Personnel Accountability
- Geo Select
- Northbound Interface
- Dynamic Frequency Blocking

LaaS IMW includes the following licenses to test NEW functionality:

- 100 Group Management Licenses
- 100 Messaging Licenses

The following Spares have also been included:

- FRE: DL380 G10 HD
- DAS
- DL380 Power Supply
- 2930F 48 Port Switch
- 2930F 24 Port Switch
- Mini GBIC
- Fiber Cable

The proposed LaaS has also been provisioned to support the following features and operation:

- SmartConnect
- SmartLocate
- ViQi
- Cirrus (Cloud based Network Management)
- Command Central Aware

Internetworking Firewall (qty 2) are included to provide secure connectivity to support the above features.

Clarification 1: *License ID's for the G Series site controller and the Base Radio; Those are no charge licenses that are attached to those equipment; site controller and the GTR base station. You already have that equipment and so no need to add those licenses again. That equipment can be connected to the Lab Test core.*

Clarification 2: *MSI is providing one CSSI license with the LaaS. Once the Critical Connect Demo is complete and MPSCS purchases Critical Connect, the demo Critical Connect System will go into lab facility and can be used as the ISSI interface. The Lab will at that point have the ISSI and CSSI to test non-Mototrola systems. The use of Critical Connect services will still be required to purchase monthly subscriptions as outlined in the pricing section of this proposal.*

Exclusions:

RF site(s), devices, consoles and associated support are not included as part of this solution.

1.3 INSTALLATION REQUIREMENTS

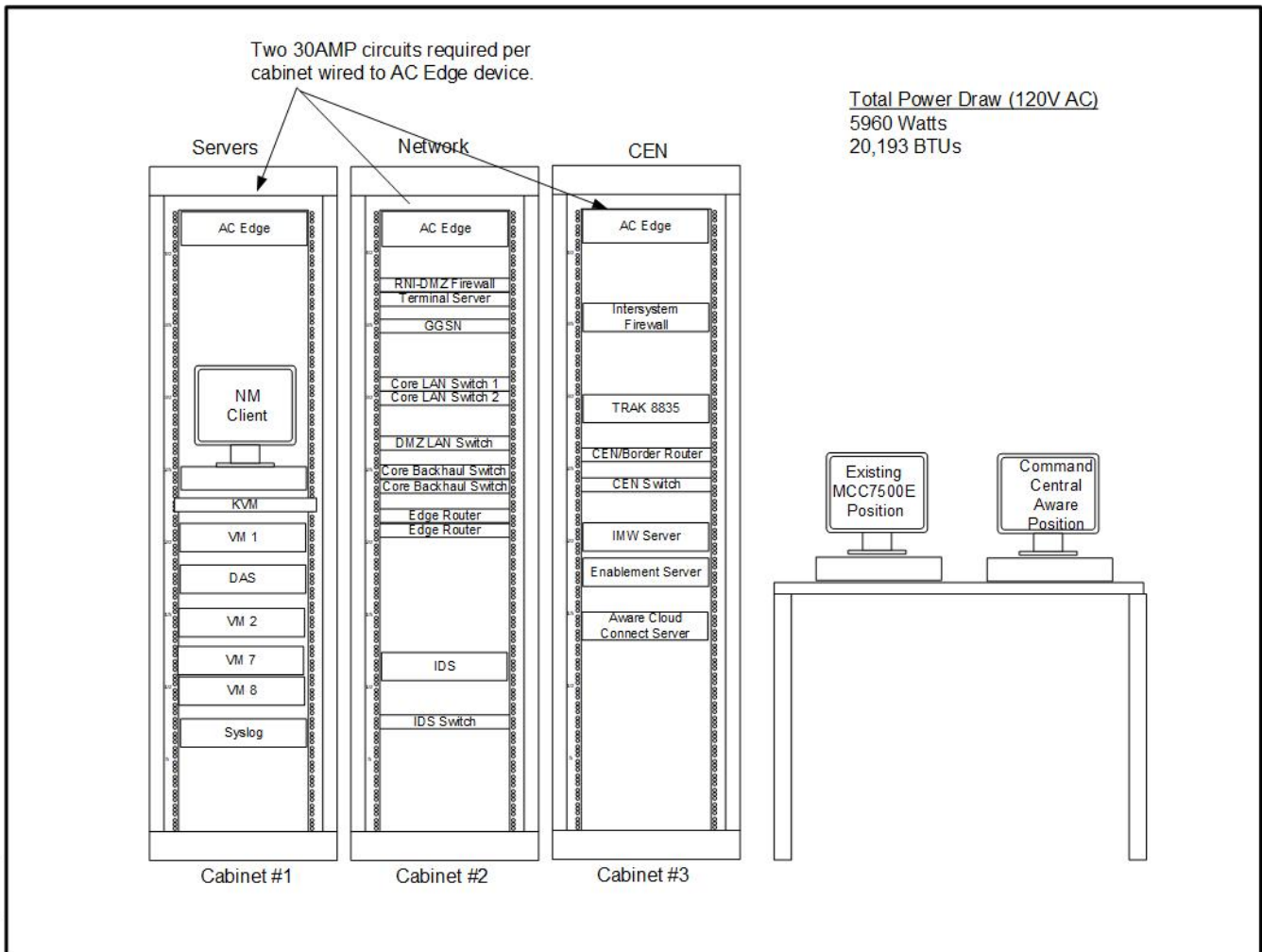
Motorola Solutions will install and configure the Test Core in the Lab based upon the agreed-to floor plans. A cabinet/rack drawing for the new Lab equipment is included. All equipment will be installed in a neat and professional manner, employing a standard of workmanship consistent with Motorola Solutions' R56 installation standards and in compliance with applicable standards and regulations.

1.3.1 MPSCS Responsibilities

- Provide assistance and access to MSI personnel to offload and move equipment to the second floor Lab location
- Provide adequate floor space for the new equipment and cabinets/racks as shown in the attached rack/cabinet drawing. Ensure 3 feet of clearance in front and back of each rack/cabinet. If required, remove or relocate any existing equipment, and utilities to create space for new equipment.
- Ensure a single point system ground, of ten (10) ohms or less, is available in the Lab room and make available a grounding tie point within ten (10) feet of the-Motorola-supplied equipment cabinets.
- Supply and install required circuits described below in the existing electrical distribution panel and wire to Motorola supplied cabinets. Ensure AC feed input power is sized to support the additional circuits required below.
 - Provide Qty 2 30 amp 120V AC circuits per cabinet and wire to AC Edge PDU's in each cabinet.
 - Provide adequate power to the Aware Client
 - Provide additional circuits for future equipment that may be added in the Lab. A mutually acceptable number will be determined jointly between MPSCS and MSI.
- Provide UPS backup power for the new LaaS equipment sized to meet total power draw as shown on the cabinet/rack drawing.

- Provide long term generator backup power to backup new LaaS equipment.
- Provide a dedicated owner or point of contact for the Lab to work with the MSI resource
- Provide dedicated internet connectivity, which would be used for either security patching, software updates and/or cloud service testing. The connectivity that is being used in site 1102 should be sufficient.

Figure 1-1: Master Rack Diagram



1.4 COMMANDCENTRAL AWARE PRODUCT DESCRIPTION

CommandCentral Aware provides a complete operating picture, integrating intelligence in the command center to remotely assist officers in the field. CommandCentral Aware can create a situational awareness front through consolidation of disparate systems and data such as radio locations into a single interface with the ability to expand data sources when the agency is ready to include incidents from CAD, camera feeds, alerts and voice.

The CommandCentral Aware package proposed for the Test Lab supports monitoring location of GPS enabled portable and mobile radios in a single map view. The Aware package is a cloud based solution offering the ability to view this map anywhere and on multiple device types; workstation, laptop, smartphone, or tablet. A single workstation Aware client has been included to be located in the Lab.

CommandCentral Aware also has the ability to connect to Computer Aided Dispatch (CAD), Call Handling, Video Management Systems (VMS), Automatic License Plate Reader (ALPR) and other software platforms, enhancing incident response by integrating these multiple disparate systems into a unified public safety workflow. CommandCentral Aware provides the ability to correlate information and events across these types of multiple systems; radio, video surveillance, sensors, alarms, analytics, CAD, Records, and Mapping/GPS location.

The ability to interface to these different types of data sources and information would enable your member agencies to monitor activity from anywhere, act with necessary context, collaborate without distraction, respond quickly to escalating incidents, enhance response with real time video, streamline video management and agency workflows.

The capability for these other systems can be added to the proposed Aware package in the future when desired for testing and validation.

More detail on the package included is described below.

The CommandCentral Solution design for the MPSCS Lab project includes the following:

CommandCentral Aware Location Software Solution:

- Licenses for CommandCentral Aware Location on PTT (Qty. 10)
- AccuWeather service
- Agency ESRI Data Sets Integration
- Location
 - Inter/Intra-Agency Group configuration
 - IMW Software Upgrade
 - IMW licenses including: location, presence and group management
- Man-down alerts and emergency button
- Emergency Alerts: APX radio button press, man-down and vehicle impact

Hardware Components:

- One (1) CloudConnect server hardware

Professional Services Includes:

- Field Engineering for installation and integration of the CloudConnect server. and configuration of the CommandCentral Aware application.



- CommandCentral Aware on-line training through the Motorola Learning Management System (LMS).

1.5 MAPPING DESCRIPTION

CommandCentral Aware provides the consolidated, map-based common operating picture needed to enhance decision-making at any part of your operation. You can view all of your location-based data together, on a single map display.

Geospatial Event Mapping - See up to 3000 unit/device locations (only 10 radio locations will be mapped for this Lab project), field personnel status and location, open-source data alerts, sensors and more, visualized on a map that can be customized with any of your agency's other data layers.

Event Monitors - Personnel status and location, open source data alerts, visualized on a map (i.e. Esri online, Esri server, or static map layers) that can be modified with any of your agency's other data layers.

Geographical Information System (GIS) Integration - Map display utilizes Esri ArcGIS online or ArcGIS Server map services provided by the Customer.

Data Layer Panel - Each data layer source can be shown or hidden based on selecting or deselecting it in the data layer panel.

Event Information Display - Details associated with each icon on the map can be viewed in an event information display upon clicking the icon.

1.6 LOCATION ON PTT DESCRIPTION

CommandCentral Aware maps GPS enabled land mobile radios (ASTRO 25 radios). The location solution supports the following capabilities:

- User & Resource Location - All available agency sources of location information and related metadata are ingested from land mobile radio (LMR) devices to pinpoint the location for vehicles and responders.
- Affiliation of Users, Devices and Units - A user can be affiliated with multiple devices (both broadband and LMR). Multiple users and their devices can be affiliated with a unit.
- Location on PTT and On Request.
- Location on Emergency (emergency button press and man down).
- Stale Location or Not Reporting Indication.

1.7 LOCATION ON PTT FEATURES

The chart below will help you to better understand the capabilities that your agency can leverage when using the CommandCentral Aware Map to track your unit's location. This chart highlights the Location-on-PTT Offer for CommandCentral Aware. Location-on-PTT is a subscription based offer that is easily deployed with any up-to date ASTRO® P25 system.












	LMR LOCATION
	LOCATION ON DEMAND OR REQUEST
	LOCATION ON PTT
	AFFILIATION OF USERS, DEVICES, UNITS, GROUPS
	WORKFLOW CONFIGURATION
	EMERGENCY ALERTS (APX BUTTON PRESS, MAN DOWN, VEHICLE IMPACT)
	ESSENTIAL SERVICE
	ASTRO 25 RESPONDER LOCATION
	AGENCY ESRI DATA SETS INTEGRATION

Figure 1-2: LoPTT Features

1.8 GEOGRAPHIC INFORMATION SYSTEM (GIS) DATA SET INTEGRATION

CommandCentral Aware integrates with your hosted GIS data sets from Esri ArcGIS Server or ArcGIS online. The geospatial information contained within these data sets are core to the overall visualization of the intelligent map display. This adds to the common operating picture to enhance workflow details driven by geography and metadata contained within these data sets.

Esri's powerful geospatial engine within CommandCentral Aware is used to automatically invoke spatial queries to inform the user of nearby items, refine geographic boundaries and focus attention on location to orientate those responding. Utilizing the geospatial processing induces an intelligent driven analysis and help to eliminate additional noise on the map to not distract from the concentrated area of concern.

Example data sets may include (but not limited to):

- The ability to refine the data displayed based on geographic area defined per user (i.e. by Area, Beat, Sector, Precinct, Zone, Quadrant).
- Find nearby entities by predefined distance (i.e. closest responder to an emergency event).
- Determining road blockades caused by traffic jams, flooded roadways, or barricades.

SECTION 2

LAAS SERVICES

2.1 SERVICES OVERVIEW

Motorola will support to ensure the LaaS is operating at optimal levels and available for MPSCS to perform testing activities. The proposed offering consists of the following specific services:

- Technical Support.
- Network and Security Update Services (SUS)
- System Upgrade Service (SUAI)
- Annual Preventative Maintenance.
- Maintenance related onsite support

These services will be delivered to MPSCS through the combination of local service personnel and a centralized team within our Solutions Support Center (SSC), which operates on a 24 x 7 x 365 basis; The collaboration between these service resources, all of who are experienced in the maintenance of mission-critical networks, will enable a swift analysis of any network issues, an accurate diagnosis of root causes, and a timely resolution and return to normal network operation.

2.2 TECHNICAL SUPPORT

Centralized support will be provided by Motorola Solutions' support staff, located at our Service Desk and Solutions Support Center (SSC). These experienced personnel will provide direct service and technical support through a combination of Service Desk telephone support, technical consultation and troubleshooting through the SSC. Motorola Solutions will provide Service Desk response as a single point of contact for all support issues, including communications between MPSCS, third-party subcontractors and manufacturers, and Motorola Solutions. When MPSCS's personnel call for support, the Service Desk will record, track, and update all Service Requests, Change Requests, and Service Incidents using our Customer Relationship Management (CRM) system. The Service Desk is responsible for documenting MPSCS's inquiries, requests, concerns, and related tickets; tracking and resolving issues; and ensuring timely communications with all stakeholders based on the nature of the incident.

As tickets are opened by the Service Desk, issues that require specific technical expertise and support will be routed to our Solutions Support Center (SSC) system technologists for Technical Support, who will provide telephone consultation and troubleshooting capabilities to diagnose and resolve infrastructure performance and operational issues.

Motorola Solutions' recording, escalating, and reporting process applies ISO 90001 and TL 9000-certified standards to the Technical Support calls from our contracted customers, reflecting our focus on maintaining mission-critical communications for the users of our systems.

2.3 SECURITY UPDATE SERVICE (SUS)

The proposed Security Patch Installation Service will provide MPSCS with pre-tested security updates, pre-tested and installed by Motorola ST on MPSCS's LaaS system. When appropriate, Motorola Solutions will make these updates available to outside vendors in order to enable them to test each patch, and will incorporate the results of

those third-party tests into the updates before installation on MPSCS's network. Once an update is fully tested and ready for deployment in MPSCS's system, Motorola Solutions will locally install it onto MPSCS's system, and notify MPSCS that the patch has been successfully installed. *In general, MSI would be responsible for the network security of the new LaaS but expect to work with MPSCS personnel on governance, process and protocol. To our knowledge the lab does not have internet access at this point but we are asking for it in order to perform off premise patching, updates and upgrades (when possible), therefore at this point all updates and patching is on-premise until we get internet access to perform it remotely. MSI is proposing to do remote security patching (Moto-patch) and will work with MPSCS on the final methodology, process, schedule and any bandwidth requirements.* If there are any recommended configuration changes, warnings, or workarounds, Motorola Solutions will provide detailed documentation along with the updates on the website.

2.4 SYSTEM UPGRADE SERVICE (SUAI)

With our proposed Network Updates Service through the SUAI program, Motorola Solutions commits to sustain MPSCS's ASTRO 25 system through a SUAI program of software and hardware updates aligned with the Live Production system and the ASTRO 25 platform lifecycle. *Motorola's service and upgrade operations team is committing to upgrade the Lab system 6 months prior to the live system being upgraded. This assumes these upgrade discussions are happening a minimum of 8 months prior to the live system being upgraded and the new system upgrade is available.* This comprehensive approach to technology sustainment will ensure that MPSCS has access to the latest available standard features, as well as the opportunity to incorporate optional features through the purchase of hardware and/or software licenses. Updates and expansion of system components will optimize the availability of repair services, and will enable MPSCS to add RF sites, dispatch positions, data subsystems, network management positions, and other elements to increase capacity and processing capability.

Motorola Solutions will minimize any interruption to system operation during each network update in cooperation with MPSCS's personnel.

2.5 PREVENTIVE MAINTENANCE

Annual Preventive Maintenance Service provides proactive, regularly scheduled operational testing and alignment of infrastructure and network components to ensure that they continually meet original manufacturer specifications. Certified field technicians perform hands-on examination and diagnostics of network equipment on a routine and prescribed basis.



2.6 NETWORK HARDWARE REPAIR

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

2.7 MAINTENANCE ONSITE SUPPORT

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

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

Core Master Site Tasks*	Lead Responsibility	Assistance
Verification Testing of Products Chosen by MPSCS	MPSCS	MSI
Validation Testing of Products Chosen by MPSCS	MPSCS	MSI
Core Configuration, provisioning and programming	MSI	MPSCS
Technical Support Service Desk 7X24	MSI	
Security Update Service	MSI	
Network Patch Management	MSI	
Preventive Maintenance	MSI	
Field Technical Maintenance	MSI	
System Enhancement Releases (SER)	MSI	
<ul style="list-style-type: none"> ▪ SUA II - Up to one system upgrade every two years ▪ Core SMA/Software Maintenance Agreement ▪ Core Hardware Refresh ▪ Core Upgrade Related HW/SW Implementation 	MSI	

**RF site(s), devices, consoles are not included as part of this solution.*

SECTION 3

LAB AS A SERVICE (LAAS) TECHNICAL RESOURCE

3.1 OVERVIEW

Provide oversight and lead the product, software and feature testing in collaboration with Michigan's Public Safety Communications System (MPSCS) team members. Below is a general overview of the position:

- In cooperation and collaboration with MPSCS, lead and set up the future testing procedures, approval processes and documentation requirements for both Motorola Solutions (MSI) and MPSCS
- In cooperation with both MPSCS and MSI personnel, establish, document and update overall MPSCS and MSI technical network and architectural diagrams and drawings for the current system (as-builts) and what the future state of the system may need to be for proper growth and capacity requirements.
- Prioritize the testing of features, software, technology, updates, upgrades and equipment replacement with MSI and MPSCS personnel
- Actively partner, communicate and collaborate with MSI field teams to ensure they are updated on roadmap and testing priorities, progress and approval of products, services and technologies. MSI field teams include but not limited to:
 - Pre and Post sale engineering teams
 - System Technologists
 - Project Management
 - Product teams
 - Service teams
- Partner with MSI internal research and development (R&D), systems integration testing (SIT) and product teams and provide MPSCS voice of customer (VOC) feedback for product development and rollout.
- Work closely with the following MPSCS/State of Michigan teams to establish technology roadmap and VOC priorities:
 - Engineering Team
 - Software/Data Team
 - Architectural and Network Team
 - Radio Programming Team
 - Network Control Center Team
 - Field Services Teams
 - Cyber Security Team
- Have an overall understanding of the MSI products, services and technologies currently on the MPSCS.

- Land Mobile Radio (LMR) System and Landscape
- Premier One(P1)/Computer Aided Dispatch (CAD)
- Backhaul - Nokia
- Third party partners such as NICE, Genesis, MCM, CompassCom, Kodiak, WAVE,
- Train and participate in classes, forums and/or training to understand the future products, technology, software and services
 - Land Mobile Radio (LMR) System and Landscape
 - Premier One(P1)/Computer Aided Dispatch (CAD)
 - Backhaul - Nokia
 - Third party partners such as NICE, Genesis, MCM, CompassCom, Kodiak, WAVE,
- *MPSCS will have final approval of this resource and will participate in the interview process.*

3.1.1 Specific Duties

- Carry out and actively participate / support tests / trials, integration tests, certification tests, diagnostic tests, etc.
- Assist and advise MPSCS personnel in setting up tests and trials to validate new features and functionality to be performed on the Test core prior to deploying on the production system.
- Act as the Field technical resource during SUAII upgrades performed by Motorola Upgrade Operations.
- Participate in response and restoral to remediate functional issues with the test core.
- Support the design and deploy test benches (e. g. Key Performance Index measurement - KPI)
- Report development / technical advice / task assistance / trials
- Act as technical link between Motorola Solutions and MPSCS (question, etc.).
- Serve as focal point & catalyst for the resolution of product and system problems in complex communications and information systems
- Develop new methods to improve performance, ease of installation, diagnostics, quality, and cycle time of complex systems
- Technical support to engineering and expertise. (If required)
- Perform preventative maintenance routines to ensure proper system operation with focus on trend analysis and documentation of results

3.1.2 Skills

- Expertise in configuration and testing ("pre staging / staging").
- Special skills and knowledge in the fields of radio communication (P25), and related fields (electromagnetic propagation and microwave links, VHF, UHF, and microwave radio technologies.) Familiarity with IP/MPLS, Telephony-ToIP.
- Must have knowledge of R.F. systems, such as transmitters, receivers, and antenna networks
- Must be highly computer literate with proficiency in MS Word, Excel, Powerpoint, Outlook or Gmail, and Access



- Must demonstrate knowledge in standard telephony and dedicated data circuits, as well as knowledge of packet switching techniques including MPLS.
- Training and extensive experience in configuring and testing computer networking equipment (routers, hubs, switches, etc.).
- Experience with logging recording systems, RF interfaces, wired/wireless communications systems and/or networking equipment
- Unique combinations of both multi-site RF communications system and/or computer/networking skills are required.
- Must demonstrate knowledge and experience in LAN/WAN networks, network administration and management
- Must be able to work with and update technical drawings as well as provide technical drawings as needed
- The ideal candidate must demonstrate systems experience and have a minimum of 4 years of related experience with the following equipment:
 - Motorola Base Stations (STR series, GTR series, Quantar, etc.)
 - Centracom Consoles (Gold Elite, MCC7500, MCC7100)
 - Nokia Microwave Backhaul Computer IP Networks and Configuration
 - Experience working with RF Infrastructure Technologies to include Motorola SmartZone, Console Systems, ASTRO25 Trunked equipment is strongly preferred
- The Candidate must have skills in the use of various communications test equipment including:
 - Communication System Analyzers
 - Ethernet Link test sets
 - T1 Test Sets
 - TIMS (Transmission Impairment Measurement Set)
 - Digital RF Power Meter
- Must be capable of installation of server hardware/OS and software infrastructure and troubleshooting to resolve system/application related issues.
- Applicants must be proficient with Microsoft Office products and Motorola Radio Programming Software suite.
- Must have excellent communications skills and always present a professional image.
- Must have a current, valid driver's license.
- Must be able to obtain background clearance as required by government customer

3.1.3 Education/Experience

- Engineering degree, or technical school certification, or military training.
- 2 or more years of MPSCS engineering experience
- Ideally the individual should have or be pursuing at least one network certification:
 - Network+
 - CCNA
 - NRS1

- Related certification Network + (or similar) certification.
- Eight years' technical work experience.
- Training and experience in the configuration, testing, and optimization of current Motorola two-way radio subscribers and infrastructure.

SECTION 4

PROPOSAL PRICING

Motorola pricing is based on a complete system solution. The addition or deletion of any component(s) may subject the total system price to modifications.

4.1 PROPOSAL SUBSCRIPTION PRICING

	Year 1	Year 2	Year 3	Year 4	Year 5
LaaS Annual Fee	\$655,000	\$674,650	\$694,890	\$715,736	\$737,208

5. MSPCS Review

Motorola will provide to the State's MPSCS reports and data as requested. MPSCS Subject Matter Experts (SME's) will meet annually to review the progress and the volume of lab simulations that have been conducted to ascertain that the program is working as intended. Motorola will work with the State to implement any changes determined to be necessary to make this program viable.

MA# 190000001544



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

SCHEDULE B – PRICING

	Component	October 1, 2019	October 1, 2020	October 1, 2021	October 1, 2022	October 1, 2023	October 1, 2024	October 1, 2025	October 1, 2026	October 1, 2027	October 1, 2028	TOTAL
MPSCS ASTRO LIFECYCLE	System Upgrade Agreement II (SUA II)	\$ 4,666,781.89	\$ 5,119,186.80	\$ 5,570,726.31	\$ 5,900,187.68	\$ 6,460,906.70	\$ 6,502,411.06	\$ 6,545,043.90	\$ 6,589,066.01	\$ 6,634,415.11	\$ 6,681,002.78	\$ 60,669,728.24
	Security Update Services (SUS)	\$ 100,785.87	\$ 103,809.45	\$ 106,923.73	\$ 118,189.84	\$ 121,735.54	\$ 125,387.60	\$ 135,019.65	\$ 139,070.24	\$ 143,242.35	\$ 147,539.62	\$ 1,241,703.89
	Technical Support (TS)	\$ 252,878.41	\$ 260,464.76	\$ 268,278.70	\$ 296,546.12	\$ 305,442.50	\$ 314,605.77	\$ 338,773.22	\$ 348,936.41	\$ 359,404.51	\$ 370,186.64	\$ 3,115,517.03
	OPSOC	\$ 34,839.75	\$ 35,884.94	\$ 36,961.49	\$ 40,855.97	\$ 42,081.65	\$ 43,344.10	\$ 46,673.71	\$ 48,073.92	\$ 49,516.14	\$ 51,001.63	\$ 429,233.31
	Business Relationship Manager (BRM)	\$ 260,000.00	\$ 267,800.00	\$ 275,834.00	\$ 284,109.02	\$ 292,632.29	\$ 301,411.26	\$ 310,453.60	\$ 319,767.21	\$ 329,360.22	\$ 339,241.03	\$ 2,980,608.62
	TOTAL	\$ 5,315,285.92	\$ 5,787,145.95	\$ 6,258,724.23	\$ 6,639,888.63	\$ 7,222,798.68	\$ 7,287,159.79	\$ 7,375,964.08	\$ 7,444,913.79	\$ 7,515,938.33	\$ 7,588,971.70	\$ 68,436,791.09
MPSCS PREMIER**	PremierOne CAD		\$ 106,678.14	\$ 109,878.36	\$ 119,812.29	\$ 123,406.92	\$ 127,108.85	\$ 135,644.68	\$ 139,714.22	\$ 143,905.79	\$ 148,222.50	\$ 1,154,371.75
	PremierMDC	\$ 162,778.86	\$ 150,358.48	\$ 154,869.30	\$ 171,187.28	\$ 176,322.96	\$ 181,612.64	\$ 195,563.48	\$ 201,430.32	\$ 207,472.88	\$ 213,696.68	\$ 1,815,292.88
	Upgrade - Hardware / Software / Services		\$ 142,848.92	\$ 142,848.92	\$ 153,301.28	\$ 153,301.28	\$ 153,301.28	\$ 160,269.52	\$ 160,269.52	\$ 160,269.52	\$ 160,269.52	\$ 1,386,679.76
	TOTAL	\$ 162,778.86	\$ 399,885.54	\$ 407,596.58	\$ 444,300.85	\$ 453,031.16	\$ 462,022.77	\$ 491,477.68	\$ 501,414.06	\$ 511,648.19	\$ 522,188.70	\$ 4,356,344.39
MPSCS Lab	Lab as A Service (5 Year Agreement)		\$ 655,000.00	\$ 674,650.00	\$ 694,890.00	\$ 715,736.00	\$ 737,208.00					\$ 3,477,484.00
	TOTAL		\$ 655,000.00	\$ 674,650.00	\$ 694,890.00	\$ 715,736.00	\$ 737,208.00					\$ 3,477,484.00
	GRAND TOTAL	\$ 5,478,064.78	\$ 6,842,031.49	\$ 7,340,970.81	\$ 7,779,079.48	\$ 8,391,565.84	\$ 8,486,390.56	\$ 7,867,441.76	\$ 7,946,327.85	\$ 8,027,586.52	\$ 8,111,160.40	\$ 76,270,619.48
MPSCS Existing Credits	Credit #1 - System Manager	(\$ 154,291.00)										(\$ 154,291.00)
	Credit #2 - WAVE Activation Fee	(\$ 1,814.40)										(\$ 1,814.40)
	Credit #3 - WAVE Hosting	(\$ 6,900.00)										(\$ 6,900.00)
	Credit #4 - Subscriber Activation	(\$ 53,750.00)										(\$ 53,750.00)
	GRAND TOTALS OF CREDITS	(\$ 216,755.40)										

** CAD Workstations NOT included in pricing



STATE OF MICHIGAN PROCUREMENT

DTMB Central Procurement Services

525 W. Allegan Street, 1st Floor NE
Lansing, MI 48933

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **19000001544**

between

THE STATE OF MICHIGAN

and

CONTRACTOR	Motorola Solutions, Inc
	500 W. Monroe St.
	Chicago, IL 60661
	Rich Uslan
	616-438-1942
	rich.uslan@motorolasolutions.com
	CV0016903

STATE	Program Manager	Kate Jannereth	DTMB
		517-881-1031	
		jannerethk@michigan.gov	
STATE	Contract Administrator	Valerie Hiltz	DTMB
		517-249-0459	
		hiltzv@michigan.gov	

CONTRACT SUMMARY

DESCRIPTION: Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment, Maintenance and Upgrades, and Ancillary Systems Products

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
October 1, 2019	December 31, 2029	None	December 31, 2029
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45		As per Delivery Order	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input checked="" type="checkbox"/> P-card <input type="checkbox"/> Payment Request (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
<p>This Master Agreement Serves as an Order with regard to Maintenance and Support, for services as indicated in Schedule A, Section 4.1.A Price Terms and Section 5.1.A.1 Authorizing Document, and per terms, conditions and specifications of this contract.</p> <p>For all other Products and Services THIS IS NOT AN ORDER. Orders will be placed directly by the State Agency via the authorized document, established in Schedule A, Section 5.1.A.2 Authorizing Documents, and per terms, conditions and specification of this contract.</p>			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			\$99,900,000.00

FOR THE CONTRACTOR:

Motorola Solutions, Inc.
Company Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Jared Ambrosier, Enterprise Sourcing Director
Name & Title

DTMB, Central Procurement Services
Agency

September 26, 2019
Date



STATE OF MICHIGAN

STANDARD CONTRACT TERMS

Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

This STANDARD CONTRACT ("**Contract**") is agreed to between the State of Michigan (the "**State**") and Motorola Solutions, Inc. ("**Contractor**" or "Motorola"), a Delaware corporation. This Contract is effective on October 1, 2019 ("**Effective Date**"), and unless terminated, expires on December 31, 2029.

1. **Definitions.** For the purposes of this Contract, the following terms have the following meanings:

"**Accept**" has the meaning set forth in **Section 20**.

"**Acceptance**" has the meaning set forth in **Section 20**.

"**Affiliate**" of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

"**Allegedly Infringing Materials**" has the meaning set forth in **Section 34**.

"**Business Day**" means a day other than a Saturday, Sunday or other day on which the State is authorized or required by Law to be closed for business.

"**Business Owner**" is the individual appointed by the agency buyer to (a) act as the agency's representative in all matters relating to the Contract, and (b) co-sign off on notice of Acceptance. The Business Owner will be identified in the Statement of Work.

"**Change**" has the meaning set forth in **Section 5**.

"**Change Notice**" has the meaning set forth in **Section 5**.

"**Change Proposal**" has the meaning set forth in **Section 5**.

"**Change Request**" has the meaning set forth in **Section 5**.

"**Confidential Information**" has the meaning set forth in **Section 38.a**.



“**Configuration**” means State-specific changes made to the Software without Source Code or structural data model changes occurring.

“**Contract**” has the meaning set forth in the preamble.

“**Contract Activities**” refers to the includes the Services, Deliverables, delivery of commodities, or other contractual requirements set forth in **Schedule A – Statement of Work**, including any subsequent Statement(s) of Work, that the Contractor agrees to provide and the State agrees to purchase pursuant to the terms of this Contract.

“**Contract Administrator**” is the individual appointed by each party to (a) administer the terms of this Contract, and (b) approve any Change Notices under this Contract. Each party’s Contract Administrator will be identified in the Statement of Work.

“**Contractor**” has the meaning set forth in the preamble.

“**Contractor’s Bid Response**” means the Contractor’s proposal submitted in response to the State’s requests to obtain Contract Activities.

“**Contractor Personnel**” means all employees of Contractor or any Permitted Subcontractors involved in the performance of Services hereunder.

“**Deliverables**” means all materials, including, but not limited to Software, Documentation, written materials and commodities, that Contractor is required to or otherwise does provide to the State under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in **Schedule A - Statement of Work**.

“**Dispute Resolution Procedure**” has the meaning set forth in **Section 54**.

“**Documentation**” means all generally available documentation relating to the Software, including all user manuals, operating manuals and other instructions, specifications, documents and materials, in any form or media, that describe any component, feature, requirement or other aspect of the Software or Hosted Services (as defined in **Schedule D**), including any functionality, testing, operation or use thereof.

“**DTMB**” means the Michigan Department of Technology, Management and Budget.

“**Effective Date**” has the meaning set forth in the preamble.

“**Equipment**” means the hardware components that the State purchases from Contractor under this Contract.

“**Fees**” means collectively all fees collected by the Contractor pursuant to the terms of this Contract.



“**Financial Audit Period**” has the meaning set forth in **Section 41**.

“**Force Majeure**” has the meaning set forth in **Section 53**.

“**HIPAA**” has the meaning set forth in **Section 46**.

“**Intellectual Property Rights**” means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable Law in any jurisdiction throughout the world.

“**Key Personnel**” means any Contractor Personnel identified as key personnel in **Schedule A – Statement of Work**.

“**Law**” means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree or other requirement or rule of any federal, state, local or foreign government or political subdivision thereof, or any arbitrator, court or tribunal of competent jurisdiction.

“**Loss or Losses**” means all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

“**Maintenance Release**” means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide to its licensees from time to time during the Term, which may contain, among other things, error corrections, enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

“**New Version**” means any new version of the Software that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

“**Permitted Subcontractor**” has the meaning set forth in **Section 13**.



“**Person**” means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

“**Pricing**” means any and all fees, rates and prices payable under this Contract, including pursuant to any Schedule or Exhibit hereto.

“**Pricing Schedule**” means the schedule attached as **Schedule B**, setting forth the Fees, rates and Pricing payable under this Contract.

“**Project Manager**” is the individual appointed by each party to (a) monitor and coordinate the day-to-day activities of this Contract, and (b) for the State, to cosign off on its notice of Acceptance of the Deliverables. Each party’s Project Manager will be identified in the Statement of Work.

“**Representatives**” means a party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

“**Software**” means Contractor’s software set forth in the Statement of Work, and any Maintenance Releases or New Versions provided to the State and any Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract and the License Agreement.

“**Services**” means any of the services Contractor is required to or otherwise does provide under this Contract, **Schedule A** - Statement of Work, **Schedule C** - Software Terms for On-site Hosting (if applicable), and **Schedule E** – Contractor Hosted Software and Services (if applicable).

“**Source Code**” means the human readable source code of the Software to which it relates, in the programming language in which the Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to understand, build, operate, support, maintain and develop modifications, upgrades, updates, adaptations, enhancements, new versions and other derivative works and improvements of, and to develop computer programs compatible with, the Software.

“**Site**” means the physical location designated by the State in, or in accordance with, this Contract or the Statement of Work for delivery or installation of the Contract Activities.

“**State**” means the State of Michigan.

“**State Data**” has the meaning set forth in **Section 37**.

“**State Materials**” means all materials and information, including equipment, documents, data, know-how, ideas, methodologies, specifications, software,



content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

“**Statement of Work**” means any statement of work entered into by the parties and attached as a schedule to this Contract. The initial Statement of Work is attached as **Schedule A**, and subsequent Statements of Work shall be sequentially identified and attached as Schedules A-1, A-2, A-3, etc.

“**Stop Work Order**” has the meaning set forth in **Section 28**.

“**Term**” has the meaning set forth in the preamble.

“**Third Party**” means any Person other than the State or Contractor.

“**Transition Period**” has the meaning set forth in **Section 32**.

“**Transition Responsibilities**” has the meaning set forth in **Section 32**.

“**Unauthorized Removal**” has the meaning set forth in **Section 15**.

“**Unauthorized Removal Credit**” has the meaning set forth in **Section 15**.

“**Warranty Period**” means the periods set forth in **Section 23**.

“**Work Product**” Refers to any data compilations, reports, and other media, materials, or other objects or works of authorship created or produced by the Contractor as a result of an in furtherance of performing the services required by this Contract.

- 2. Duties of Contractor.** Contractor must perform the Services and provide the Deliverables described in **Schedule A – Statement of Work**. An obligation to provide delivery of any commodity is considered a service and is a Contract Activity.

Contractor must furnish all labor, equipment, materials, and supplies necessary for the performance of the Contract Activities, and meet operational standards, unless otherwise specified in **Schedule A**.

Contractor must also be clearly identifiable while on State property by wearing identification issued by the State, and clearly identify themselves whenever making contact with the State.

- 3. Statement(s) of Work.** Contractor shall provide the Contract Activities pursuant to Statements of Work entered into under this Contract. No Statement of Work shall be effective unless signed by each party’s Contract Administrator. The term of each Statement of Work shall commence on the parties’ full execution of the Statement



of Work and terminate when the parties have fully performed their obligations. The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the parties and attached as a schedule to this Contract. The State shall have the right to terminate such Statement of Work as set forth in **Sections 29** and **30**. Contractor acknowledges that time is of the essence with respect to Contractor's obligations under each Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statements of Work is strictly required.

4. **Statement of Work Requirements.** Each Statement of Work may include the following: (a) names and contact information for Contractor's Contract Administrator, Project Manager and Key Personnel; (b) names and contact information for the State's Contract Administrator, Project Manager and Business Owner; (c) a detailed description of the Services to be provided under this Contract, including any training obligations of Contractor; (d) a detailed description of the Deliverables to be provided under this Contract; and (e) a detailed description of all State Resources, if any, required to complete the Implementation Plan, if such a Plan is necessary.
5. **Change Control Process.** The State may at any time request in writing (each, a "Change Request") changes to the Statement of Work, including changes to the Contract Activities (each, a "Change"). Upon the State's submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this **Section 5**. No Change will be effective until the parties have executed a Change Notice. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with the Statement of Work pending negotiation and execution of a Change Notice. Contractor will use commercially reasonable efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to the State. However, the State will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.
6. **Notices.** All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

If to State:	If to Contractor:
--------------	-------------------



Valerie Hiltz 525 W. Allegan St, 1st Floor, NE PO Box 30026 Lansing, MI 48913 hiltzv@michigan.gov 517-249-0459	Motorola Solutions, Inc. 500 W. Monroe St. 37 th Floor Attn: Legal Department Chicago, IL 60661
---	--

7. **Performance Guarantee.** Contractor must always have financial resources sufficient, in the opinion of the State, to ensure performance of the Contract and must provide proof upon request. The State may require a performance bond (as specified in Schedule A) if, in the opinion of the State, it will ensure performance of the Contract. If State requires a performance bond, Contractor may make a corresponding adjustment to its pricing to cover the costs of the bond.

8. **Insurance Requirements.** Contractor must maintain the insurances identified below and is responsible for all deductibles. All required insurance must: (a) protect the State from claims that may arise out of, are alleged to arise out of, or result from Contractor's or a subcontractor's performance; (b) be primary and noncontributing to any comparable liability insurance (including self-insurance) carried by the State; and (c) be provided by a company with an A.M. Best rating of "A-" or better, and a financial size of VII or better.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
<u>Minimum Limits:</u> \$1,000,000 Each Occurrence Limit \$1,000,000 Personal & Advertising Injury Limit \$2,000,000 General Aggregate Limit \$2,000,000 Products/Completed Operations <u>Deductible Maximum:</u> Contractor shall be solely responsible for Deductible.	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds using endorsement CG 20 10 04 13, or both CG 2010 04 13and CG 2037 04 13.



Umbrella or Excess Liability Insurance

<p><u>Minimum Limits:</u> \$5,000,000 General Aggregate</p> <p>Total Commercial Liability limits may be evidenced in any combination of Primary and Umbrella or Excess Liability.</p>	<p>Contractor must have their policy follow form.</p>
---	---

Additional insurance requirements are continued on page 11.



Automobile Liability Insurance	
<u>Minimum Limits:</u> \$1,000,000 Per Accident	Contractor must have their policy: (1) endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds; and (2)
	include Hired and Non-Owned Automobile coverage.
Workers' Compensation Insurance	
<u>Minimum Limits:</u> Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
<u>Minimum Limits:</u> \$500,000 Each Accident \$500,000 Each Employee by Disease \$500,000 Aggregate Disease.	

Professional Liability (Errors and Omissions) Insurance, including Privacy and Security Liability (Cyber Liability)	
<u>Minimum Limits:</u> \$3,000,000 Each Occurrence \$3,000,000 Annual Aggregate	Professional Liability (Errors and Omissions) Insurance policy shall include the following coverage “E&O-MPL-Primary includes coverage for Professional and Technology Based Services, Technology Products, Information Security and Privacy and Multimedia and Advertising Liability.”

If any of the required policies provide **claims-made** coverage, the Contractor must: (a) provide coverage with a retroactive date before the effective date of the contract or the beginning of Contract Activities; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the Contract Activities;



and (c) if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the contract effective date, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

Contractor must: (a) provide insurance certificates to the Contract Administrator, containing the agreement or delivery order number, at Contract formation and within 20 calendar days of the expiration date of the applicable policies; (b) require that subcontractors maintain the required insurances contained in this Section; (c) notify the Contract Administrator within 5 business days if any insurance is cancelled; and (d) waive all rights against the State for damages covered by insurance where permitted. Failure to maintain the required insurance does not limit this waiver.

This Section is not intended to and is not to be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

- 9. Administrative Fee and Reporting.** Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract including transactions with the State (including its departments, divisions, agencies, offices, and commissions with the exception of sales to the MPSCS office or reimbursements from the MPSCS office), MiDEAL members, MPSCS members provided they are MiDEAL members, and other states (including governmental subdivisions and authorized entities). Administrative fee payments must be made by check payable to the State of Michigan and mailed to:

Department of Technology, Management and Budget
Cashiering
P.O. Box 30681
Lansing, MI 48909

Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports should be mailed to MiDeal@michigan.gov.

The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

- 10. Extended Purchasing Program.** This contract is extended to MiDEAL and MPSCS members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of



MiDEAL members is available at www.michigan.gov/mideal. Upon written agreement between the State and Contractor, this contract may also be extended to other states (including governmental subdivisions and authorized entities). MPSCS members are those members who have registered with and are recognized as users on the MPSCS by DTMB MPSCS.

If extended, Contractor must supply all Contract Activities at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions.

Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

- 11. Independent Contractor.** Contractor is an independent contractor and assumes all rights, obligations and liabilities set forth in this Contract. Contractor, its employees, and agents will not be considered employees of the State. No partnership or joint venture relationship is created by virtue of this Contract. Contractor, and not the State, is responsible for the payment of wages, benefits and taxes of Contractor's employees and any subcontractors. Prior performance does not modify Contractor's status as an independent contractor.
- 12. Intellectual Property Rights.** Contractor hereby acknowledges that the State is and will be the sole and exclusive owner of all right, title, and interest in the Work Product produced as part of the Contract Activities, and all associated intellectual property rights, if any. In general, Work Product constitutes works made for hire as defined in Section 101 of the Copyright Act of 1976. To the extent any Work Product, and related intellectual property do not qualify as works made for hire under the Copyright Act, Contractor will, and hereby does, immediately on its creation, assign, transfer and otherwise convey to the State, irrevocably and in perpetuity, throughout the universe, all right, title and interest in and to the Work Product, including all intellectual property rights therein. Contractor also irrevocably waives any and all claims Contractor may have now or hereafter have in any jurisdiction to so called "moral rights" or rights of *droit moral* with respect to the Work Product. If Contract Activities includes the purchase or use of software, such purchase, use, or access to Software shall be subject to **Schedules C** and **D** of this Contract.

Contractor is neither developing nor creating any intellectual property under this Agreement, and any such work performed by Contractor will be performed under a separate, mutually agreed upon development agreement.



- 13. Subcontracting.** Contractor will not, without the prior written approval of the State, which consent may be given or withheld in the State's sole discretion, engage any Third Party to perform Services. The State's approval of any such Third Party (each approved Third Party, a "**Permitted Subcontractor**") does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will: (a) be responsible and liable for the acts and omissions of each such Permitted Subcontractor (including such Permitted Subcontractor's employees who, to the extent providing Services or Deliverables, shall be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees; (b) name the State a third party beneficiary under Contractor's Contract with each Permitted Subcontractor with respect to the Services; (c) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and (d) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.
- 14. Staffing.** Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits. The State's Contract Administrator may require Contractor to remove or reassign personnel by providing a notice to Contractor.
- 15. Key Personnel.** If, in the sole discretion of the State, Key Personnel are required to complete the Contract Activities, such Key Personnel shall be identified in **Schedule A - Statement of Work**. The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State's Project Manager, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include



replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under **Section 29**.

It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 29**, Contractor will issue to the State an amount set forth in **Schedule A – Statement of Work** (each, an “**Unauthorized Removal Credit**”).

- 16. Background Checks.** Pursuant to Michigan law, all agencies subject to IRS Pub. 1075 are required to ask the Michigan State Police to perform fingerprint background checks on all employees, including Contractor and Subcontractor employees, who may have access to any database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or Subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018. Upon request, Contractor must perform background checks on all employees and subcontractors and its employees prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks.
- 17. Assignment.** Contractor may not assign this Contract to any other party without the prior approval of the State, which will not be unreasonably withheld. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other party. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.
- 18. Change of Control.** Contractor will notify within 30 days of any public announcement, or otherwise once legally permitted to do so, the State of a change in Contractor's organizational structure or ownership. For purposes of this Contract, a change in control means any of the following: (a) a sale of more than 50% of Contractor's stock; (b) a sale of substantially all of Contractor's assets; (c)



a change in a majority of Contractor's board members; (d) consummation of a merger or consolidation of Contractor with any other entity; (e) a change in ownership through a transaction or series of transactions; (f) or the board (or the stockholders) approves a plan of complete liquidation. A change of control does not include: 1) any consolidation or merger effected exclusively to change the domicile of Contractor, or 2) any transaction or series of transactions principally for bona fide equity financing purposes; or 3) any acquisition that does not materially change control or ownership.

In the event of a change of control, Contractor must require the successor to assume this Contract and all of its obligations under this Contract.

- 19. Ordering.** Contractor is not authorized to begin performance until receipt of authorization as identified in Schedule A.
- 20. Acceptance.** Contract Activities are subject to inspection and testing by the State within fifteen (15) business days of the State's receipt of them ("**State Review Period**"), unless otherwise provided in Schedule A. If the Contract Activities are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the Contract Activities are accepted but noted deficiencies must be corrected; or (b) the Contract Activities are rejected. If the State finds material deficiencies, it may: (i) reject the Contract Activities without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with **Section 29**, Termination for Cause.

Within 10 business days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any Contract Activities in accordance with this Contract, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable Contract Activities to the State. If acceptance with deficiencies or rejection of the Contract Activities impacts the content or delivery of other non-completed Contract Activities, the parties' respective Program Managers must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct deficiencies in accordance with the time response standards set forth in this Contract.

If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or in part. The State, or a third party identified by the State, may perform the Contract Activities and recover the difference between the cost to cure and the Contract price.

- 21. Delivery.** Contractor must deliver all Contract Activities F.O.B. destination, within the State premises with transportation and handling charges paid by Contractor,



unless otherwise specified in Schedule A. All containers and packaging become the State's exclusive property upon acceptance.

- 22. Risk of Loss and Title.** Until final acceptance, title and risk of loss or damage to Contract Activities remains with Contractor. Title to software will not pass to State at any time under any circumstances. Contractor is responsible for filing, processing, and collecting all damage claims. The State will record and report to Contractor any evidence of visible damage. If the State rejects the Contract Activities, Contractor must remove them from the premises within 10 calendar days after notification of rejection. The risk of loss of rejected or non-conforming Contract Activities remains with Contractor. Rejected Contract Activities not removed by Contractor within 10 calendar days will be deemed abandoned by Contractor, and the State will have the right to dispose of it as its own property. Contractor must reimburse the State for costs and expenses incurred in storing or effecting removal or disposition of rejected Contract Activities.
- 23. Warranty Period.** The warranty period, if applicable, for Contract Activities is a fixed period commencing on the date specified in **Schedule A or below in this Section.**
- 23.1 EQUIPMENT WARRANTY.** During the Warranty Period, Contractor warrants that the Equipment under normal use and service will be free from material defects in materials and workmanship. If System Acceptance is delayed beyond six (6) months after shipment of the Equipment by events or causes beyond Contractor's control, this warranty expires eighteen (18) months after the shipment of the Equipment.
- 23.2 SOFTWARE WARRANTY.** Except as described in the Schedule E and unless otherwise stated in the Software License Agreement, during the Warranty Period, Contractor warrants the Software in accordance with the warranty terms set forth in the Software License Agreement and the provisions of this Section that are applicable to the Software. If System Acceptance is delayed beyond six (6) months after shipment of the Contractor Software by events or causes beyond Contractor's control, this warranty expires eighteen (18) months after the shipment of the Contractor Software. **Nothing in this Warranty provision is intended to conflict or modify the Software Support Policy. In the event of an ambiguity or conflict between the Software Warranty and Schedule E, the Schedule E governs.**
- 23.3 EXCLUSIONS TO EQUIPMENT AND SOFTWARE WARRANTIES.** These warranties do not apply to: (i) defects or damage resulting from: use of the Equipment or Software in other than its normal, customary, and authorized



manner; accident, liquids, neglect, or acts of God; testing, maintenance, disassembly, repair, installation, alteration, modification, or adjustment not provided or authorized in writing by Contractor; State's failure to comply with all applicable industry and OSHA standards; (ii) breakage of or damage to antennas unless caused directly by defects in material or workmanship; (iii) Equipment that has had the serial number removed or made illegible; (iv) batteries (because they carry their own separate limited warranty) or consumables; (v) freight costs to ship Equipment to the repair depot; (vi) scratches or other cosmetic damage to Equipment surfaces that does not affect the operation of the Equipment; and (vii) normal or customary wear and tear.

- 23.4 **SERVICE WARRANTY.** During the Warranty Period, Contractor warrants that the Services will be provided in a good and workmanlike manner and will conform in all material respects to the applicable Statement of Work. Services will be free of defects in materials and workmanship for a period of ninety (90) days from the date the performance of the Services are completed. State acknowledges that the Deliverables may contain recommendations, suggestions or advice from Contractor to State (collectively, "recommendations"). Contractor makes no warranties concerning those recommendations, and State alone accepts responsibility for choosing whether and how to implement the recommendations and the results to be realized from implementing them.
- 23.5 **WARRANTY CLAIMS.** To assert a warranty claim, State must notify Contractor in writing of the claim before the expiration of the Warranty Period. Upon receipt of this notice, Contractor will investigate the warranty claim. If this investigation confirms a valid Equipment or Software warranty claim, Contractor will (at no additional charge to State) repair the defective Equipment or Contractor Software or replace it with the same or equivalent product or, as an option of last resort, refund the price of the defective Equipment or Contractor Software. These actions will be the full extent of Contractor's liability for the warranty claim (in conjunction with the State's right to terminate this Contract for breach, where applicable, and any remedy set forth in the Service Level Agreement). In the event of a valid Services warranty claim, State's sole remedy (in conjunction with the State's right to terminate this Contract for breach and any remedy set forth in the Service Level Agreement) is to require Contractor to re-perform the nonconforming Service or to refund the fees paid for the non-conforming Service. If this investigation indicates the warranty claim is not valid, then Contractor may invoice State for responding to the claim on a time and materials basis using Contractor's then current labor rates. Repaired or replaced product is



warranted for the balance of the original applicable warranty period. All replaced products or parts will become the property of Contractor.

- 23.6 ORIGINAL END USER IS COVERED. These express limited warranties are extended by Contractor to the original user purchasing the System or Services for commercial, industrial, or governmental use only, and are not assignable or transferable.
- 23.7 DISCLAIMER OF OTHER WARRANTIES. THESE WARRANTIES ARE THE COMPLETE WARRANTIES FOR THE EQUIPMENT AND CONTRACTOR SOFTWARE PROVIDED UNDER THIS AGREEMENT AND ARE GIVEN IN LIEU OF ALL OTHER WARRANTIES. CONTRACTOR DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.
- 24. Terms of Payment.** Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Contract Activities performed as specified in **Schedule A or a mutually agreed upon and executed Change Notice**. Invoices must include an itemized statement of all charges. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services purchased under this Agreement are for the State's exclusive use. All prices are exclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Contract Activities. Contractor's acceptance of final payment by the State constitutes a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still disputed.

The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at <http://www.michigan.gov/SIGMAVSS> to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment. Without prejudice to any other right or remedy it may have, the State reserves the



right to set off at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

- 25. Payment Disputes.** The State may withhold from payment any and all payments and amounts the State disputes in good faith, pending resolution of such dispute, provided that the State: (a) timely renders all payments and amounts that are not in dispute; notifies Contractor of the dispute prior to the due date for payment, specifying in such notice: (i) the amount in dispute; and (ii) the reason for the dispute set out in sufficient detail to facilitate investigation by Contractor and resolution by the parties; (b) works with Contractor in good faith to resolve the dispute promptly; and (c) promptly pays any amount determined to be payable by resolution of the dispute.

Contractor shall not withhold any Contract Activities or fail to perform any obligation hereunder by reason of the State's good faith withholding of any payment or amount in accordance with this **Section 25** or any dispute arising therefrom.

- 26. Liquidated Damages.** Liquidated damages, if applicable, will be assessed as described in **Schedule A**. Amounts due the State as liquidated damages may be set off against any Fees payable to Contractor under this Contract, or the State may bill Contractor as a separate item and Contractor will promptly make payments on such bills.
- 27. Stop Work Order.** The State may suspend any or all activities under the Contract at any time. The State will provide Contractor a written stop work order detailing the suspension. Contractor must comply with the stop work order upon receipt. Within 90 calendar days, or any longer period agreed to by Contractor, the State will either: (a) issue a notice authorizing Contractor to resume work, or (b) terminate the Contract or delivery order. The State will not pay for Contract Activities, Contractor's lost profits, or any additional compensation during a stop work period.
- 28. Termination for Cause.** The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State: (a) endangers the value, integrity, or security of any location, data, or personnel; (b) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; (c) engages in any conduct that may expose the State to liability; (d) breaches any of its material duties or obligations; or (e) fails to cure a breach within the time stated in a notice of breach. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

If the State terminates this Contract under this Section, the State will issue a termination notice specifying whether Contractor must: (a) cease performance



immediately, or (b) continue to perform for a specified period. If it is later determined that Contractor was not in breach of the Contract, the termination will be deemed to have been a Termination for Convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 30**, Termination for Convenience.

The State will only pay for amounts due to Contractor for Contract Activities performed by Contractor on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. The Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Contract Activities from other sources.

- 29. Termination for Convenience.** The State may immediately terminate this Contract in whole or in part without penalty and for any reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must: (a) cease performance of the Contract Activities immediately, or (b) continue to perform the Contract Activities in accordance with **Section 31**, Transition Responsibilities. If the State terminates this Contract for convenience, the State will pay all reasonable costs for State approved Transition Responsibilities in addition to any amounts owed to Contractor for shipped equipment and services performed through the date of termination.
- 30. Effect of Termination.** Upon and after the termination or expiration of this Contract or one or more Statements of Work for any or no reason: (a) Contractor will be obligated to perform all Transition Responsibilities specified in **Section 32**; (b) all licenses granted to Contractor in State Data will immediately and automatically also terminate. Contractor must promptly return to the State all State Data not required by Contractor for its Transition Responsibilities, if any; (c) Contractor will: (i) return to the State all documents and tangible materials (and any copies) containing, reflecting, incorporating, or based on the State's Confidential Information; (ii) permanently erase the State's Confidential Information from its computer systems; and (iii) certify in writing to the State that it has complied with the requirements of this **Section 31** in each case to the extent such materials are not required by Contractor for Transition Responsibilities, if any.
- 31. Transition Responsibilities.** Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 3 Years, "**Transition Period**"), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract Activities to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Contract Activities to the State or its designees. Such



transition assistance may include, but is not limited to: (a) continuing to perform the Contract Activities at the established Contract rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Contract Activities, training, equipment, software, leases, reports and other documentation, to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return to the State all materials, data, property, and confidential information provided directly or indirectly to Contractor by any entity, agent, vendor, or employee of the State; (d) transferring title in and delivering to the State all completed or partially completed deliverables prepared under this Contract as of the Contract termination date, which does not include Software as title to Software does not pass to the State at any time; and (e) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, "**Transition Responsibilities**"). This Contract will automatically be extended through the end of the transition period.

- 32. General Indemnification.** Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to: (a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract; (b) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable); and (c) any negligent, willful or intentional acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the satisfaction of the State, demonstrate its financial ability to carry out these obligations.

The State is entitled to: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; (iii) employ its own counsel; and to (iv) retain control of the defense if the State deems necessary. Contractor will not, without the State's written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. To the extent that any State employee, official, or law may be involved



or challenged, the State may, at its own expense, control the defense of that portion of the claim.

Any litigation activity on behalf of the State, or any of its subdivisions under this Section, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

- 33. Infringement Indemnification and Remedies.** Contractor must indemnify, defend and hold harmless the State, its departments, divisions, agencies, offices, commissions, officers and employees, from and against all losses, liabilities, damages (including taxes), and all related costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties) incurred in connection with any action or proceeding threatened or brought against the State to the extent that the action or proceeding is based on a claim that any piece of equipment, software, commodity or service manufactured by the Contractor or its subcontractors, or the operation of the equipment, software, commodity or service, or the use or reproduction of any documentation provided with the equipment, software, commodity or service infringes any patent, copyright, or trademark of any person or entity.

In addition, should the equipment, software, commodity, or service, or its operation, become or in the State's or Contractor's opinion be likely to become the subject of a claim of infringement, the Contractor must at the Contractor's sole expense (i) procure for the State the right to continue using the equipment, software, commodity or service or, if the option is not reasonably available to the Contractor, (ii) replace or modify to the State's satisfaction the same with equipment, software, commodity or service of equivalent function and performance so that it becomes non-infringing, or, if the option is not reasonably available to Contractor, (iii) accept its return by the State with appropriate credits to the State against the Contractor's charges and reimburse the State for any losses or costs incurred as a consequence of the State ceasing its use and returning it.

Notwithstanding the foregoing, the Contractor has no obligation to indemnify or defend the State for, or to pay any costs, damages or attorneys' fees related to, any claim based upon (i) equipment developed based on written specifications of the State; (ii) use of the equipment in a configuration other than implemented or approved in writing by the Contractor, including, but not limited to, any modification of the equipment by the State, if such modification or nonapproved use is the basis for the claimed infringement; or (iii) the combination, operation, or use of the equipment with equipment or software not supplied by the Contractor under this Contract, unless the Documentation of Specifications refers to a combination with such equipment or software (without directing the State not to perform such a



combination or such combination achieves functionality described in the Documentation or Specifications) and neither the Documentation or Specifications directs the State not to perform such combination.

In no event will Contractor's liability resulting from its indemnity obligation to the State extend in any way to royalties payable on a per use basis or the State's revenues, or any royalty basis other than a reasonable royalty based upon revenue derived by Contractor from State from sales or license of the infringing equipment, software, commodity or service.

34. Limitation of Liability and Disclaimer of Damages.

- (a) Disclaimer of Damages. NEITHER PARTY WILL BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.
- (b) Limitation of Liability. IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY TO THE OTHER PARTY UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED ONE AND ONE HALF (1.5) TIMES THE MAXIMUM THE AGGREGATE CONTRACT PRICE. As used in this clause, the term "Aggregate Contract Price" means the total price for the initial Term and all renewal terms of this Contract.
- (c) Exceptions. Subsections (a) (Disclaimer of Damages) and (b) (Limitation of Liability) above, will not apply to: (i) Contractor's obligation to indemnify under **Sections 33 and 34** of this Contract; (ii) any loss or claim to the extent the loss or claim is covered by a policy of insurance maintained, or required by this Contract to be maintained, by Contractor; and (iii) damages arising from either party's recklessness, bad faith, or intentional misconduct.
- (d) Nothing herein will be construed to waive any law regarding sovereign immunity, or any other immunity, restriction, or limitation on recovery provided by law.

NOTWITHSTANDING THE FOREGOING, IN NO EVENT WILL CONTRACTOR'S AGGREGATE LIABILITY UNDER THIS CONTRACT



WHEN CONTRACTING WITH MiDEAL AND MPSCS MEMBERS (I.E., NOT THE STATE OR A STATE AGENCY), REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THE APPLICABLE PROPOSAL/QUOTE OR STATEMENT OF WORK.

- 35. Disclosure of Litigation, or Other Proceeding.** Contractor must notify the State within 14 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding (collectively, “**Proceeding**”) involving Contractor, a subcontractor, or an officer or director of Contractor or subcontractor, that arises during the term of the Contract, including: (a) a criminal Proceeding; (b) a parole or probation Proceeding; (c) a Proceeding under the Sarbanes-Oxley Act; (d) a civil Proceeding involving: (1) a claim that might reasonably be expected to adversely affect Contractor’s viability or financial stability; or (2) a governmental or public entity’s claim or written allegation of fraud; or (e) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract.
- 36. State Data.** All data and information provided to Contractor by or on behalf of the State, and all data and information derived therefrom, is the exclusive property of the State (“State Data”); this definition is to be construed as broadly as possible. Upon request, Contractor must provide to the State, or a third party designated by the State, all State Data within 10 calendar days of the request and in the format requested by the State. Contractor will assume all costs incurred in compiling and supplying State Data. No State Data may be used for any marketing purposes. If Contractor is in possession of any State Data, it will comply with State policies and procedures regarding Data Privacy and Information Security.
- 37. Non-Disclosure of Confidential Information.** The parties acknowledge that each party may be exposed to or acquire communication or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties. The provisions of this Section survive the termination of this Contract.
- a. Meaning of Confidential Information. For the purposes of this Contract, the term “**Confidential Information**” means all information and documentation of a party that: (a) has been marked “confidential” or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked “confidential” or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked “confidential” or with words of similar meaning; and, (c) should reasonably be recognized as confidential information of the disclosing party. The term “Confidential Information” does not



include any information or documentation that was: (a) subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

- b. Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to a subcontractor is permissible where: (a) use of a subcontractor is authorized under this Contract; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the subcontractor's responsibilities; and (c) Contractor obligates the subcontractor in a written contract to maintain the State's Confidential Information in confidence. At the State's request, any employee of Contractor or any subcontractor may be required to execute a separate agreement to be bound by the provisions of this Section.
- c. Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract and each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.
- d. Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the



case of the State, at the sole election of the State, the immediate termination of this Contract or any Statement of Work, in accordance with this Contract, corresponding to the breach or threatened breach.

- e. Surrender of Confidential Information upon Termination. Upon termination of this Contract or a Statement of Work, in whole or in part, each party must, within 5 calendar days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control; provided, however, that Contractor must return State Data to the State following the timeframe and procedure described further in this Contract. Should Contractor or the State determine that the return of any Confidential Information is not feasible, such party must destroy the Confidential Information and must certify the same in writing within 5 calendar days from the date of termination to the other party. However, the State's legal ability to destroy Contractor data may be restricted by its retention and disposal schedule, in which case Contractor's Confidential Information will be destroyed after the retention period expires.

38. Reserved.

39. Reserved.

- 40. Records Maintenance, Inspection, Examination, and Audit.** The State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to the Contract through the term of the Contract and for 4 years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Audit Period, Contractor must retain the records until all issues are resolved.

Within 30 calendar days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor's premises or any other places during normal business hours where Contract Activities are being performed, and examine, copy, and audit all directly pertinent records related to this Contract. Contractor must cooperate and provide reasonable assistance. Contractor books and records provided to State pursuant to this provision shall not be used, duplicated or disclosed to any other third party without the express written permission of Contractor. In no circumstances will Contractor be required to create or maintain documents not kept in the ordinary course of Contractor's business operations, nor will Contractor be required to



disclose any information, including but not limited to product cost data, which it considers confidential or proprietary. If any financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of the Contract must be paid or refunded within 45 calendar days.

This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Contract Activities in connection with this Contract.

- 41. Warranties and Representations.** Contractor represents and warrants: (a) Contractor is the owner or licensee of any Contract Activities that it licenses, sells, or develops and Contractor has the rights necessary to convey title, ownership rights, or licensed use; (b) Contractor will perform the Contract Activities in a timely, professional, safe, and workmanlike manner consistent with standards in the trade, profession, or industry; (c) Contractor will meet or exceed the performance and operational standards, and specifications of the Contract; (d) Contractor will provide all Contract Activities in good quality, with no material defects; (e) Contractor will not interfere with the State's operations; (f) all Contract Activities are delivered free from any security interest, lien, or encumbrance and will continue in that respect; (g) Contractor must assign or otherwise transfer to the State or its designee any manufacturer's warranty for the Contract Activities; (h) the Contract Activities are merchantable and fit for the specific purposes identified in the Contract; (i) the Contract signatory has the authority to enter into this Contract; (l) all information furnished by Contractor in connection with the Contract fairly and accurately represents Contractor's business, properties, finances, and operations as of the dates covered by the information, and Contractor will inform the State of any material adverse changes; (m) all information furnished and representations made in connection with the award of this Contract is true, accurate, and complete, and contains no false statements or omits any fact that would make the information misleading; and that (n) Contractor is neither currently engaged in nor will engage in the boycott of a person based in or doing business with a strategic partner as described in 22 USC 8601 to 8606. A breach of this Section is considered a material breach of this Contract, which entitles the State to terminate this Contract under **Section 29**, Termination for Cause. If Contract Activities includes purchase, use, or access to software, Contractor must agree to additional Warranties and Representations found in **Schedules C** or **D** of this Contract, as applicable.
- 42. Conflicts and Ethics.** Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything



of value; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. Contractor must immediately notify the State of any violation or potential violation of these standards. This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Contract Activities in connection with this Contract.

- 43. Compliance with Laws.** Contractor must comply with all applicable federal, state and local laws, rules and regulations.
- 44. ADA Compliance.** The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. Contractor's Service Software must comply, where relevant, with level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.
- 45. HIPAA Compliance.** The State and Contractor must comply with all obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if reasonably necessary to keep the State and Contractor in compliance with HIPAA.
- 46. Prevailing Wage.** Contractor must comply with prevailing wage requirements, to the extent applicable to this Contract.
- 47. Reserved.**
- 48. Nondiscrimination.** Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq.*, the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq.*, and [Executive Directive 2019-09](#). Contractor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex (as defined in Executive Directive 2019-09), height, weight, marital status, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position. Breach of this covenant is a material breach of this Contract.
- 49. Unfair Labor Practice.** Under MCL 423.324, the State may void any Contract with a Contractor or subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.



- 50. Governing Law.** This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Contractor must appoint agents in Michigan to receive service of process.
- 51. Non-Exclusivity.** Nothing contained in this Contract is intended nor will be construed as creating any requirements contract with Contractor. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Contract Activities from other sources.
- 52. Force Majeure.** Neither party will be in breach of this Contract because of any failure arising from any disaster or acts of god, or other event(s), that are beyond their control and without their fault or negligence. Each party will use commercially reasonable efforts to resume performance. Contractor will not be relieved of a breach or delay caused by its subcontractors. If immediate performance is necessary to ensure public health and safety, the State may immediately contract with a third party.
- 53. Dispute Resolution.** The parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the parties' respective Contract Administrators or Program Managers. Such referral must include a description of the issues and all supporting documentation. The parties must submit the dispute to a senior executive if unable to resolve the dispute within 15 business days. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance.

Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' senior executive and either concludes that resolution is unlikely or fails to respond within 15 business days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This Section does not limit the State's right to terminate the Contract.

- 54. Media Releases.** News releases (including promotional literature and commercial advertisements) pertaining to the Contract or project to which it relates must not be made without prior written State approval, and then only in accordance with the explicit written instructions of the State.



- 55. Website Incorporation.** The State is not bound by any content on Contractor's website unless expressly incorporated directly into this Contract.
- 56. Schedules.** All Schedules and Exhibits that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule A, Attachment 1	SUAll Agreement
Schedule A, Attachment 2	SUS Agreement
Schedule A, Attachment 3	PremierOne Maintenance and Support Agreement
Schedule A, Attachment 4	OPSOC Service Overview
Schedule A, Attachment 5	Technical Support
Schedule A, Attachment 6	Business Relationship Manger (BRM)
Schedule A, Attachment 7	Security Addendum
Schedule A, Attachment 8	Customer Support Plan
Schedule A, Exhibit 1	Quotations Sample Document
Schedule B	Pricing and Fees
Schedule C	Software Terms for On-site Hosting
Schedule D	Software License Agreement for On-site Hosting
Schedule E	Software Support Policy
Schedule F	Federal Provisions Addendum
Schedule G	System Configuration

- 57. Entire Agreement and Order of Precedence.** This Contract, which includes Schedule A – Statement of Work, and schedules and exhibits which are hereby expressly incorporated, is the entire agreement of the parties related to the Contract Activities. This Contract supersedes and replaces all previous understandings and agreements between the parties for the Contract Activities. If there is a conflict between documents, the order of precedence is: (a) first, this Contract, excluding its schedules, exhibits, and Schedule A – Statement of Work; (b) second, Schedule A – Statement of Work as of the Effective Date; and (c) third, schedules expressly incorporated into this Contract as of the Effective Date. NO TERMS ON CONTRACTOR'S INVOICES, ORDERING DOCUMENTS, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH



ANY OF THE CONTRACT ACTIVITIES WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE OR ITS AUTHORIZED USERS FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE, EVEN IF ACCESS TO OR USE OF THE CONTRACT ACTIVITIES REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

- 58. Severability.** If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.
- 59. Waiver.** Failure to enforce any provision of this Contract will not constitute a waiver.
- 60. Survival.** The provisions of this Contract that impose continuing obligations, including warranties and representations, termination, transition, insurance coverage, indemnification, and confidentiality, will survive the expiration or termination of this Contract.



STATE OF MICHIGAN

Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

SCHEDULE A STATEMENT OF WORK CONTRACT ACTIVITIES

BACKGROUND

The Michigan's Public Safety Communications System (MPSCS) was established in order to provide for a unified, statewide radio communication system which may be utilized by all emergency entities that wish to use it statewide.

There are currently over 1800 different emergency agencies that are members of this system. This number is expected to increase as new counties and agencies come on board.

INTENT

This contract is the vehicle by which the State of Michigan, its Agencies and MiDeal and/or MPSCS members, may maintain, upgrade, and integrate into the public safety radio system including software and hardware.

SCOPE

The Contractor shall provide all necessary management, personnel, equipment, tools, materials, software, supervision, training, installation and other items, including but not limited to, for the provision of:

- A. Security Updates Services and System Upgrade Agreements inclusive of;
 - 1. equipment maintenance and upgrades to ancillary system products; and
 - 2. software necessary for the security, upgrade, upkeep and refresh of the MPSCS.
- B. Tech Support.
- C. Motorola brand P25 Two-Way Radios and other associated radio system hardware, accessories and furniture which may be utilized for use on and compatible with the MPSCS system.
- D. Motorola brand non-P25 Two-Way Radios and other associated radio system hardware, accessories and furniture which may be utilized for use outside of the MPSCS system.
- E. Future new technology and integration into, and the refresh of the MPSCS.



REQUIREMENTS

1. General Requirements

- A. This Master Agreement is established for use by the State of Michigan, and its MiDeal and/or MPSCS members.
 - 1. The Contractor agrees to make the same proposal terms and price, exclusive of any possible rebates, incentives, freight and transportation fees, available to State Agency, MiDeal and/or MPSCS members.
 - 2. The State of Michigan will not incur any direct liability with respect to specifications, delivery, payment, or any other aspect of purchases by MiDeal and/or MPSCS members.
 - 3. The Contractor will not include the costs, nor bill any State Agency or MiDeal and/or MPSCS member for maintenance, security and/or support already covered by the State under this contract.
- B. For integrations into the MPSCS network, this contract may only be utilized by Michigan public safety entities who have executed an MPSCS pre-integration agreement prior to final sale from contractor. The MPSCS Director reserves the right to waive this step if deemed appropriate. This waiver will be provided in writing to the entity and the Contractor. The Contractor will work directly and separately with the MiDeal and/or MPSCS members concerning the placement of orders, deliveries, disputes, invoicing and payment.
 - 1. The State of Michigan will not be held liable for any costs or damages incurred by the MiDeal and/or MPSCS member.
 - 2. The State of Michigan will not be liable for any cost associates with work established or products sold in MiDeal and/or MPSCS member contracts without the prior written consent of the State.
 - 3. The Contractor will not sell any solutions to be integrated into the MPSCS system that have not been approved by MPSCS for use on the system.
- C. The Contractor will comply with the MPSCS Technical Book of Standards which has been provided to the Contractor by the Program Manager and will be updated as necessary.

1.1. Deliverables, Products and Services

- A. System Upgrades via System Upgrades Agreement (SUA II) See **Schedule A, Attachment 1**.
- B. Ongoing Security via Security Update Service (SUS). See **Schedule A, Attachment 2**.
- C. Equipment and Ancillary Products which will be categorized into the following categories:
 - 1. **Mobile and Portable**. Includes but are not limited to:
 - a. Mobile Radio- which is a fixed mount unit installed into a vehicle.



- b. Portable Radio- which are personal radios
 - c. Consolette Radio- which are at dispatch centers or established for back up using 120v
2. **Fixed Stations.** These are the large rack mounted radios located at radio tower sites, and receivers.
3. **Dropship.** Includes non-Motorola manufactured equipment. These items may include, but are not limited to:
 - a. Microwave Equipment
 - b. Antenna Systems
 - c. Site Shelters
 - d. Console Furniture
 - e. Third party hardware or software

Please Note: drop ship items may or may not be supported by the Contractor.
Please refer to quotations or proposals.
4. **Consoles.** Includes the 911 dispatch consoles.
5. **ASTRO and SmartZone Equivalent.** Includes the system infrastructure hardware, software and software licenses, located at the system master sites, which run the P25 Radio System.
6. **Fixed Network Equipment.** Includes all system infrastructure IP networking hardware, including but not limited to:
 - a. Routers
 - b. Switches
 - c. Firewalls
7. **Spare Parts.** To repair any items sold.
8. **Accessories and Aftermarket.** Includes but is not limited to such items as:
 - a. Belt clips
 - a. Remote speaker mics
 - b. Batteries
9. **PSA PremierOne (P1) /CAD P1 Mobile/PMDC.** PSA stands for Public Safety Applications and PremierOne (P1) is the Motorola product brand; CAD stands for Computer Aided Dispatch, P1 Mobile is the vehicular CAD application, and PMDC (Premier Mobile Data Computer) is a separate mobile application associated with CAD. This category includes but is not limited to such items as:
 - a. CAD systems hardware and software
 - b. Records management software
 - c. Jail management software
 - d. Mobile applications including P1 Mobile and PMDC



10. If a product is being discontinued or support will no longer be available, the Contractor will provide to the State or MiDeal and/or MPSCS member notification as to the changes.

D. Subsystems including but not limited to:

1. ASTRO25, See **Attachment 1- SUAll Agreement and Attachment 2- SUS Agreement**
2. Premier One PSA/CAD, See **Attachment 3- PremierOne Maintenance and Support Agreement**
3. OPSOC, See **Attachment 4- OPSOC Service Overview**
4. Tech Support. See **Attachment 5- Technical Support**

1.2. Motorola Warranties

Please see Standard Terms Section 23.

1.3. Third Party Warranties, Support and Maintenance

After the initial warranty period concludes for components sold under this contract but not manufactured by the Contractor, the State and MiDeal and/or MPSCS members may elect to contract directly with third party manufacturers for extended service coverage. If contracted directly, consideration of impacts such as proper personnel certification, integration complexities, and interdependence of components is highly recommended.

1.4. Recall Requirements and Procedures

Critical product notifications will be made via Contractor's Motorola Technical Note (MTN) process.

- A. MTN bulletins will be emailed to the State and MiDeal and/or MPSCS contacts who register through the Technical Note portal at:
https://www.motorolasolutions.com/en_us/support/technical-notifications.html.
- B. Requirements and procedures for each MTN will be included with the MTN notification.

1.5. Quality Assurance Program

- A. **Quality Assurance Plan.** The Contractor will establish for each project a Quality Assurance Plan (QAP) which will provide a framework for the successful implementation and completion of projects from pre-sale through delivery of the final solution and transition to on-going service and maintenance activities. The Contractor's QAP may be refined as mutually agreed upon by the State and the Contractor throughout this contract and for each specific project. In order to maintain and assure quality, the following quality inspection points are identified:
 1. System design review
 2. System design documentation
 3. Site development and construction
 - a. Civil work completed
 - b. Tower construction



- c. Equipment shelter foundations
- d. Equipment shelter installation
- e. Grounding and bonding
- f. Electrical installation
- 4. Equipment staging
- 5. Equipment inspection and inventory
- 6. Steps of inspection throughout the implementation process
 - a. Before installing electronic equipment
 - b. After installation of electronic equipment
 - c. Before installation of antennas
 - d. After installation of antennas
- 7. As-built documentation
- 8. Final acceptance

B. **Quality Audits.** The Contractor will perform quality audits on a regular basis which will be conducted to verify that the project team is following prescribed processes and procedures. The audits take into consideration the status and importance of the processes and areas to be audited, as well as the results of any previous audits.

Quality Audit	Purpose	Planned Frequency
Documentation Reviews	Review of the project management plan and other project documentation to ensure documentation standards are being followed.	Monthly
Quality Audits	Project deliverables subject to Quality Audits and Reviews: Schedule Risk Management Plan Requirements Management Plan Communications Management Plan	Monthly

C. **Quality Assurance Controls.** Target project activities are controlled via the assurance and control methods listed in the table below:

Activity	Target	Assurance / Control
System Design	System Requirements Design Review Site Design	Compliance to requirements Joint approval



Project Management	SI Processes Status Reports Status Meetings Project Schedule Issue Tracking Log	Supervision Assessments Project Reviews Sample Inspection
Civil Work/Site Construction	Blueprints/Drawings National and Local Codes Motorola R56 Standards	Supervision Sample Inspection
Grounding/Electrical/Power Installation	Drawings/Requirements National and Local Codes Motorola R56 Standards	Supervision Sample Inspection
Activity	Target	Assurance / Control
Fixed Network Equipment (FNE) Installation	System Design Diagrams/Documentation Optimization Procedures Motorola R56 Standards	Supervision Sample Inspection
Mobile/Portable Installation	Programming Templates Installation Guides	Supervision Sample Inspection Installation Logs
System Acceptance	Coverage Testing Functional Testing Equipment Verification Feature/Functionality Testing	Sample Inspection Contract Review

Additional quality assurance and control activities include:

1. Document Control. Key project documents will be controlled through a centralized file repository. These documents have versioning control fields. Document control entails appropriate naming and versioning of project documents, templates, computer files, and other project artifacts to ensure their accuracy and relevance.
2. Factory Staging and Test. The Contractor will stage the State’s system, components, and equipment in a controlled environment and will execute system functionality tests prior to shipment,
3. Quality Reviews. Quality reviews will be scheduled to review the findings from periodic audits. They are most often conducted in conjunction with formal project meetings, whose audiences typically include members of the Contractor’s senior management.



4. Vendor Product and Service Quality. The Contractor's Global Supplier organization is responsible for identifying, vetting, and approving third-party providers of products and services. This organization reviews supplier business plans, processes, and performance on an annual or semi-annual basis, as needed.
- D. **Quality Policy.** The Contractor has committed to ensure that the effectiveness of the quality management system continually evolves, as technology and needs evolve, to meet the highest level of requirements and expectations.

1.6. Incentives

Contractor may, at its discretion, offer special incentives.

1.7. Specific Standards

A. IT Policies, Standards and Procedures (PSP)

Contractors are advised that the State has methods, policies, standards and procedures that have been developed over the years. Contractors are expected to provide proposals that conform to State IT policies and standards. All services and products provided as a result of this contract must comply with all applicable State IT policies and standards. Contractor is required to review all applicable links provided below and state compliance in their response.

Public IT Policies, Standards and Procedures (PSP):

https://www.michigan.gov/dtmb/0,5552,7-358-82547_56579_56755---,00.html

B. Acceptable Use Policy

To the extent that Contractor has access to the State's computer system, Contractor must comply with the State's Acceptable Use Policy, see http://michigan.gov/dtmb/0,4568,7-150-56355_56579_56755---,00.html. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing the State's system. The State reserves the right to terminate Contractor's access to the State's system if a violation occurs.

C. ADA Compliance

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. The State is requiring that Contractor's proposed Solution, where relevant, to level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0. Contractor may consider, where relevant, the W3C's Guidance on Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT) for non-web software and content. The State may require that Contractor complete a Voluntary Product Accessibility Template for WCAG 2.0 (WCAG 2.0 VPAT) or other comparable document for the proposed Solution.

http://www.michigan.gov/documents/dmb/1650.00_209567_7.pdf?20151026134621



1.8. Access Control and Audit

The Contractor's solution may integrate with the State's IT Identity and Access Management (IAM) environment as described in the State of Michigan Digital Strategy (http://www.michigan.gov/dtmb/0,5552,7-150-56345_56351_69611-336646--,00.html), which consist of:

- A. MILogin/Michigan Identity, Credential, and Access Management (MICAM)
An enterprise single sign-on and identity management solution based on IBM's Identity and Access Management products including, IBM Security Identity Manager (ISIM), IBM Security Access Manager for Web (ISAM), IBM Tivoli Federated Identity Manager (TFIM), IBM Security Access Manager for Mobile (ISAMM), and IBM DataPower, which enables the State to establish, manage, and authenticate user identities for the State's Information Technology (IT) systems.
- B. MILogin Identity Federation
Allows federated single sign-on (SSO) for business partners, as well as citizen-based applications.
- C. MILogin Multi Factor Authentication (MFA, based on system data classification requirements)
Required for those applications where data classification is Confidential and Restricted as defined by the 1340.00 Michigan Information Technology Information Security standard (i.e. the proposed solution must comply with PHI, PCI, CJIS, IRS, and other standards).
- D. MILogin Identity Proofing Services (based on system data classification requirements)
A system that verifies individual's identities before the State allows access to its IT system. This service is based on "life history" or transaction information aggregated from public and proprietary data sources. A leading credit bureau provides this service.

To integrate with the SOM MILogin solution, the Contractor's solution must support HTTP Headers based SSO, or SAML, or OAuth or OpenID interfaces for the SSO purposes.

1.14 SUITE Documentation

In managing its obligation to meet the above milestones and deliverables, the Contractor is required to utilize the applicable [State Unified Information Technology Environment \(SUITE\)](#) methodologies, or an equivalent methodology proposed by the Contractor.

2. Service Levels

2.1. Time Frames

- A. The Contractor will acknowledge requests for quotations within 5 business days.
- B. Timelines for deliveries shall be established in the individual DO's.

2.2. Delivery

Delivery will be expected to be made within the time frame and to the location agreed upon in the Delivery Order.



2.3. Installation

Installation will be expected within the timeframe and at the location agreed upon in the Delivery Order. Installation will be considered complete as per **Section 7, Acceptance**.

2.4. Technical Support

See **Attachment 8, Technical Support**.

2.6. Training

Training will be addressed in the statement of work for each individual project or upgrade as they occur, as necessary, and as established in the Delivery Order.

2.7. Reporting

The Contractor must submit the following reports, upon request, in a format acceptable to the State.

- A. To the Program Manager:
 - 1. Monthly Executive Status
 - 2. Monthly Sales Activity
 - 3. Project and Integration status
 - 4. List of Equipment deployed on the MPSCS inclusive of model numbers, assigned serial numbers, and warranty status.
 - 5. List of Equipment, including serial numbers, covered under the SUA
 - 6. List of Equipment, including serial numbers, covered under the SUS

- B. To the Contract Administrator:
 - 1. Quarterly Line item Sales Report inclusive of quantities and pricing.

- C. To the MiDeal Coordinator:
 - 1. As established in Standard Terms, **Section 9 Administrative Fee and Reporting**.

2.8. Meetings

The Contractor's Key Personnel will attend any meetings the State deems appropriate at the State's request.

2.9. Duplication of Services.

The Contractor will ensure that no State Agency or MPSCS member is being sold or is paying for services that are already incorporated as part of this agreement or work that MPSCS provides to its members.



2.10. Service Level Agreements (SLA's)

Subject to Section 52 of this Contract, for work performed by Contractor as part of services rendered under this agreement, the Contractor will meet the requirements and service levels established in this contract.

The State recognizes that the MPSC system is managed and maintained by State of Michigan personnel and therefore SLA credits will not be assessed in cases where at least one of the following procedures have been performed: DDP sign-off, acceptance testing and/or lab testing.

Service Level Credits may only be assessed against those services that Motorola has provided within the normal state of Michigan support.

Failure to meet the following SLA's may result in the State's assessing Service Credits:

- A. The State of Michigan reserves the right to apply a service credit of \$5,000 to the next invoice when the Contractor has six (6) or more non-critical failures (severity levels 2, 3 and 4) that are unresolved or did not meet the response times laid out in the contract in a one (1) month period.
- B. The State of Michigan reserves the right to apply a service credit of \$800.00 per hour, to the next invoice when the Contractor does not resolve or meet the response times or does not meet resolution times during a total failure (severity 1) specific to Astro, with the total service credit not to exceed \$140,000 per occurrence.
- C. All credits, as referenced in A and B above, shall not exceed, in aggregate during the term of the contract, \$1,000,000,000.

RESPONSE TIME GOAL			
Severity Level	Description	Response Time	Resolution Time
Severity 1	Total System Failure - occurs when the System is not functioning and there is no workaround; such as a Central Server is down or when the workflow of an entire agency is not functioning. This level is meant to represent a major issue that results in an unusable System, Subsystem, Product, or critical features. No work	Telephone conference within 1 Hour of initial verbal notification , Continuously.	Work around within 4 hours of initial notification, and resolution of the failure will be developed and deployed within a timeframe established in writing and mutually agreed to by MPSCS and Motorola for each incident. MPSCS will be notified within 15 minutes if the work around or final resolution plans change.



RESPONSE TIME GOAL

Severity Level	Description	Response Time	Resolution Time
	<p>around or immediate solution is available.</p> <p>A Motorola TSC Technician will respond within one hour of the request for support being logged in the issue management system. Continual effort will be maintained to restore the system or provide a viable workaround resolution. Response provided 24 x 7.</p>		
Severity 2	<p>Non-Critical Major Failure - This error level occurs when a major but non-critical element in the System is not functioning but that does not prohibit continuance of basic operations. There is usually no suitable work-around. Note that this may not be applicable to intermittent problems. This level is meant to represent a moderate issue that limits a Customer's normal use of the System, Subsystem, Product or major non-critical features.</p>	<p>Telephone conference within 3 Business Hours of initial verbal notification during normal (standard) business hours. Standard Business Day - Monday through Friday 8AM to 5PM, ET, excluding US Holidays.</p>	<p>Resolution of the failure will occur within three (3) days and resolution of the failure will be developed and deployed within a timeframe established in writing and mutually agreed to by MPSCS and Motorola for each incident.</p>
Severity 3	<p>Non-Critical Minor Failure- Non-Critical part or component failure occurs when a System component is not functioning, but the System is still useable for its intended purpose, or there is a reasonable workaround. This level is meant to represent a minor issue that does not preclude use of the System, Subsystem, Product, or critical features.</p>	<p>Telephone conference within 8 Business Hours of initial notification during normal (standard) business hours. Standard Business Day- Monday through Friday 8AM to 5PM, excluding US Holidays.</p>	<p>Resolution of the failure will occur within 10 days and resolution of the failure will be developed and deployed within a timeframe established in writing and mutually agreed to by MPSCS and Motorola for each incident.</p>



RESPONSE TIME GOAL

Severity Level	Description	Response Time	Resolution Time
Severity 4	<p>Non-Critical Minor Failure- Non-Critical part or component failure occurs when a System component is not functioning, but the System is still useable for its intended purpose, or there is a reasonable workaround. This level is meant to represent a minor issue that does not preclude use of the System, Subsystem, Product, or critical features.</p> <p>Minor issues include but are not limited to: cosmetic issues, documentation errors, general usage questions, and product or System Update requests.</p>	<p>Telephone conference within two (2) Standard Business Days of initial notification. Standard Business Day - Monday through Friday 8AM to 5PM, excluding US Holidays.</p>	<p>Resolution of the failure will occur within 15 days and resolution of the failure will be developed and deployed within a timeframe established in writing and mutually agreed to by MPSCS and Motorola for each incident.</p>

3. Staffing

3.1. Key Personnel

A. Assignment and Removal

1. See Standard Terms Section 15. Key Personnel.
2. Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under Standard Terms Section 21, Contractor will issue to the State the corresponding credits set forth below (each, an "Unauthorized Removal Credit"):
 - a. For the Unauthorized Removal of any Key Personnel designated in the applicable Statement of Work, the credit amount will be \$25,000.00 per individual if Contractor identifies a replacement approved by the State and assigns the replacement to shadow the Key Personnel who is leaving for a period of at least 30 calendar days before the Key Personnel's removal.
 - b. If Contractor fails to assign a replacement to shadow the removed Key Personnel for at least 30 calendar days, in addition to the \$25,000.00 credit specified above, Contractor will credit the State \$833.33 per calendar day for each day of the 30 calendar-day shadow period that the replacement Key Personnel does not shadow the removed Key Personnel, up to \$25,000.00 maximum per individual. The total



Unauthorized Removal Credits that may be assessed per Unauthorized Removal and failure to provide 30 calendar days of shadowing will not exceed \$50,000.00 per individual.

3. Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under Subsection iii above is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate.

A. Identified Key Personnel

The Contractor must appoint the following Key Personnel to this master agreement who will be responsible for interacting with the State and ensuring the contract and its activities meet contract requirements.

1. Contractor Representative

The Contractor must appoint a Senior Account Manager who, acting as the Contractor's Representative, will be specifically assigned to State of Michigan account, be knowledgeable on the contractual requirements, responsible for handling contract changes and will respond to State inquires within 8 business hours. The Contractor Representative or designee must be available for contact between the hours of 8am to 5 pm Eastern.

For this contract the Contractor Representative is identified as:

Senior Account Manager
Rich Uslan
Attn: Legal Department 500
West Monroe St.
37th Floor
Chicago, IL 60661 616-438-1942
rich.uslan@motorolasolutions.com

2. Business Relationship Manager

The Contractor must appoint a Business Relationship Manager who, acting as the Program Manager, will be specifically assigned and solely dedicated to the State of Michigan account, be knowledgeable on the contractual requirements and will respond to State inquiries regarding the Contract Activities, answering questions related to ordering and delivery, etc. (the "Program Manager"). This individual will respond to State inquiries within 8 business hours. The Business Relationship Manager or designee must be available for contract between the hours of 8am to 5 pm Eastern.



3.2. Non-Key Personnel

The Contractor must notify the Contract Administrator at least 10 business days before removing or assigning non-key personnel. Non-Key Personnel for this contractor are identified as:

Motorola CJIS Personnel Officer
 Kim Bales
 7237 Church Ranch Blvd Broomfield,
 CO 80021
 kimbales@motorolasolutions.com

3.3. Contract Administrator

The Contract Administrator for each party is the only person authorized to modify any terms of this Contract, and approve and execute any change under this Contract (for the State a **“Contract Administrator”**, for the Contractor a **“Contractor Representative”**):

For the State:	For the Contractor:
Valerie Hiltz 525 W. Allegan Street Lansing, MI 48833 hiltzv@michigan.gov 517-249-0459	Rich Uslan Attn: Legal Department 500 West Monroe St. 37 th Floor Chicago, IL 60661 616-438-1942 rich.uslan@motorolasolutions.com

3.4. Program Manager

The Program Manager for each party will monitor and coordinate the day-to-day activities of the Contract (for the State a **“Program Manager”**, for the Contractor a **“Business Relationship Manager”**):

For the State:	For the Contractor:
Kate Jannereth 7150 Harris Drive Dimondale, MI 48821 jannerethk@michigan.gov 517-881-1031	Robert Batis 7150 Harris Drive, Dimondale, MI 48821 bob.batis@motorolasolutions.com (989) 682.4925

3.5. Organizational Chart

- A. The Contractor will provide an overall organizational chart that details staff members, by name and title, and subcontractors that will perform work related to this contract within 10 business days of the execution of this contract.



- B. The Contractor will provide an updated Organization Chart within 10 business days as requested by the Program manager or designee.

3.6. Utilization of Subcontractors

- A. Any subcontractors will be bound by the terms of this contract. The State will not accept billing from nor make direct payments to any subcontractor.
- B. The Contractor will give the State 30 calendar days' notice if it intends to replace any subcontractor and provide the same information as required below.
- C. Any subcontractor who will have access to the MPSCS, whether physically or remotely, will provide to the Contractor a list of all employees who will be servicing this contract. The Contractor will in turn provided this list to the Program Manger on an annual basis or upon request.
- D. The Contractor will provide to the Program Manager, annually, a list of preferred and authorized Motorola Service Providers and authorized Manufacturers Representatives.

3.7. Security

- A. The Contractor will comply with the MPSCS Security Authorization Access Process and the NCC Site Access Procedure, copies of which will be provided to the Contractor by the Program Manager and updated as necessary. Any subcontractors will be bound by these same requirements.
- B. See Attachment 3- PremierOne and Attachment 7- Security Addendum regarding CJIS security requirements.

4. Pricing

- A. Pricing for this contract is as established in Schedule B.
- B. The State shall bear no costs for implementations or systems established by a MiDeal and/or MPSCS member.
- C. The State is tax exempt and will pay no taxes for products or services.

4.1. Price Term

- A. Maintenance and Support Pricing is firm fixed for the entire length of the ten base contract years for the items to follow.
 1. System Upgrade Agreement II
 2. Security Update Services
 3. Technical Support
 4. Business Relationship Manager
 5. OPSOC
 6. PMDC Support
 7. PremierOne PSA/CAD Support



- B. The Discounts Off List will remain firm and fixed for the ten base contract years. The equipment price list will be updated as published by the Contractor. See **Section 4.3. Electronic Catalog**.

4.2. Price Changes

- A. Adjustments to the SUAll and the SUS will be as negotiated. Negotiations will occur:
 - 1. During year 4 to address system changes and new contracted integrations scheduled for years six through ten; and
 - 2. No later than 2.5 years prior to the contract term expiration in preparation for a new contract.

- B. If MiDeal and/or MPSCS members add or remove equipment from the system after the Effective Date that will impact the SUAll or SUS pricing to the State, the Contractor's Program Manager will meet with the MPSCS Program Manager to discuss the changes and anticipated cost ramifications prior to quoting the MiDeal and/or MPSCS members for the proposed changes within 10 business days.
 - 1. MPSCS will review the proposed change cost against the budget and:
 - a. Confirm that the State can absorb the SUAll costs within the timeline indicated by the Contractor
 - b. Confirm that the State will not be able to absorb the SUAll costs within the timeline indicated by the Contractor but will include those costs at a future date.
 - c. A Change Notice will be executed to include the additional SUAll costs at the agreed upon time.
 - 2. If the State cannot absorb the additional SUAll costs within the proposed timeline indicated by the Contractor, the Contractor will build into their quote to the MiDeal and/or MPSCS members 's quote the costs to sustain their SUA II until the agreed upon time when the State can include those costs in their budget.
 - a. Change Notice will be executed to include the additional SUAll costs at the agreed upon time in keeping with budget approval.

- C. Should any of the scope be modified, the resulting price adjustments will be agreed upon and will remain firm fixed for the duration of the base term.

- D. The Contractor remains responsible for Contract Activities at the current price for all orders received before the mutual execution of a Change Notice indicating the start date of the new Pricing Period.

4.3 Electronic Catalog

The Contractor will provide access to the Motorola North America Product Catalog (PCAT).

- A. This access will be read only.
- B. The Contractor will provide the State with login credentials which will be utilized by the State and the MPSCS members to audit and verify current product pricing against which the Discounts Off List are placed.



4.4 Format Required for Quotations.

- A. **Quotations for Systems.** A professional quote will be required for equipment and services that are for systems requiring significant systems integration/ professional services. By providing quotes in this format, the Contractor provides a level of documentation required by governmental entities for audit purposes.
1. These quotes must be provided on the Motorola letterhead or bear the Motorola logo and shall include all the following elements:
 - a. Title Page
 - b. Table of Contents
 - c. Cover Letter – Signed by the authorized Motorola representative
 - d. System Description – including equipment and technical diagrams
 - e. Statement of Work which provides description of how the system will be implemented.
 - f. Warranty and maintenance information
 - g. Equipment list – detailed by line item including Motorola part number, quantity, description, list price, and discounted price
 - 1) Third party drop ship equipment will be broken out with line item pricing.
 - h. Professional Services List- detailed by line item including quantity, list price and discounted price.
 - i. Training- Description of training included in this proposal, if applicable.
 - j. Pricing Summary – Subtotals of equipment and Professional Services that mirrors the equipment list and pricing for install services.
 - k. Product Literature – if applicable
 - l. No additional terms or conditions, other than provided for in this contract are allowed.
 2. Quotations may be provided, at the discretion of the requestor in:
 - a. Hard copy via fax, US Postal Delivery, courier service or in person
 - b. PDF format via e-mail.
- B. **Quotations for Deliverables that are “Box Sales”.** The Contractor may provide a quote in a form format, for “Box Sales” which are those sales essentially for product with minimal amount of professional services or system integration. The quotation form must include all the elements of the sample Simple Quotation provided in **Exhibit 1 to Schedule A**. No additional terms or conditions, other than provided for in this contract are allowed.



5. Ordering

5.1. Authorizing Document

- A. The appropriate authorizing document for the Contract will be this Master Agreement and/or a Delivery Order (DO) against this Master Agreement.
 1. The following services, upgrades and maintenance are annually authorized with this Master Agreement acting as the basis of the order. **See Section 8.1.A.** for invoicing requirements:
 - a. System Upgrade Agreement II (SUAI)
 - b. Security Update Services (SUS)
 - c. Technical Support
 - d. Business Relationship Manager
 - e. OPSOC
 - f. PMDC Support
 - g. PremierOne CAD Support
 2. The appropriate authorizing document for all other contracted products or deliverables will be a DO.
- B. No verbal orders are acceptable or will be acknowledged by the State except as follow:
 1. P-Card purchases may be made as outlined in **Section 8.2.** below.
- C. MiDeal and/or MPSCS Members may use the official written document of their choosing referencing this Master Agreement.

5.2 Order Verification

The Contractor must have internal controls to identify and prevent abnormal orders, for example orders for items other than quoted, of unusually large quantities or products not normally purchased, and to ensure that individuals place orders through SIGMA for State of Michigan orders or through the appropriate purchasing paths for MiDeal members.

6. Delivery

6.1. Delivery

Contractor will make delivery of equipment as required and specified in each Delivery Order (DO).

6.2. Packaging and Palletizing

- A. Shipments must be palletized whenever possible using manufacturer's standard 4-way shipping pallets.
- B. Sensitive electronic equipment, racks and servers will be per manufacturers recommendation.



6.3 Packing Slips

Packing slips must include product description including model numbers, assigned serial numbers of equipment shipped and quantities of each.

7. Acceptance

7.1. Acceptance, Inspection and Testing

The State will use the following criteria to determine acceptance of the Contract Activities: A. Phase Acceptance/Final Acceptance (Milestone) for quoted systems and projects: Contract activities will be performed to a milestone schedule as established in the Delivery order. Acceptance will be made on milestone basis.

1. Motorola will work with the State or MiDeal and/or MPSCS team to review and accept each phase of the project as it is completed.
 - a. Unfinished work in a project phase must be recorded as a punch list item on the phase acceptance document.
 - b. Punch list items that do not interrupt system operations will not prohibit the start of the next phase of work.
 - c. At the end of the project, final acceptance is granted when all punch list items are completed.
 - d. Provide diagrams and documentation for each phase as agreed upon.
 - e. The Contractor will document punch list items, track and report to the team their progress in order to provide timely feedback on scope changes and document lessons learned.

B. Acceptance for “Box Sale” equipment: Acceptance for “box sale” equipment, defined as equipment sold outside of a system implementation, will be in keeping with acceptance outlined in **Standard Terms Section 20**.

8. Invoice and Payment

8.1. Invoice Requirements

- A. Annual services, upgrades and maintenance identified in Section 5.1.A.1. will be automatically invoiced on an annual basis.
 1. Any credits due to the State, based on the Managed Wave Broadband Solutions MWS agreement will be shown on as a line item credit against these annual charges.
- B. Invoicing for products and deliverables ordered via a DO will be based on prices established at time of order.
 1. Invoices will not be submitted until:
 - a. Product has been delivered; or
 - b. Milestone Payment: Once the Contractor has completed a milestone.
- C. All invoices submitted to the State must include:
 - a. date;
 - b. master agreement number and/or delivery order number;



- c. quantity;
- d. description of the Contract Activities;
- e. unit price; and
- f. total price.

8.2. Payment Methods

The State will make payment for Contract Activities via EFT. P-Card payment will be allowed for orders.

9. Licensing Agreement

The Contractor must provide a copy of any applicable licensing agreement.



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

**ATTACHMENT 1 to SCHEDULE A
ASTRO 25 SYSTEM UPGRADE AGREEMENT II (SUA II)**

1.0 Description of Service and Obligations

- 1.1** As system releases become available, the Contractor agrees to provide the State with the software, hardware and implementation services required to execute up to one system infrastructure upgrade in a two-year period for their ASTRO 25 system. At the time of the system release upgrade, the Contractor will provide applicable patches and service pack updates when and if available. Currently, The Contractor's service includes 3rd party SW such as [REDACTED] and any The Contractor software service packs that may be available. The Contractor will only provide patch releases that have been analyzed, pre-tested, and certified in a dedicated ASTRO 25 test lab to ensure that they are compatible and do not interfere with the ASTRO 25 network functionality.
- 1.2** The State will have, at its option, the choice of upgrading in either Year 1 or Year 2 of the coverage period. To be eligible for the ASTRO 25 SUA II, the ASTRO 25 system must be at system release 7.7 or later.
- 1.3** ASTRO 25 system releases are intended to improve the system functionality and operation from previous releases and may include some minor feature enhancements. At the Contractor's option, system releases may also include significant new feature enhancements that The Contractor may offer for purchase. System release software and hardware shall be pre-tested and certified in The Contractor's Systems Integration Test lab.
- 1.4** The price quoted for the SUAII requires the State to choose a certified system upgrade path from the list of System Release Upgrade Paths available to the State as per the system release upgrade chart referenced and incorporated in Appendix A. Should the State elect an upgrade path other than one listed in Appendix A, the State agrees that additional costs may be incurred to complete the implementation of the certified system upgrade. In this case, The Contractor agrees to provide a price quotation for any additional materials and services necessary.
- 1.5** ASTRO 25 SUA II entitles the State to past software versions for the purpose of downgrading product software to a compatible release version.



1.6 The following ASTRO 25 certified system release software for the following products are covered under this ASTRO 25 SUA II:

- 1.6.1 Servers
- 1.6.2 Workstations
- 1.6.3 Firewalls
- 1.6.4 Routers
- 1.6.5 LAN switches
- 1.6.6 MCC 7XXX Dispatch Consoles
- 1.6.7 GTR8000 Base Stations
- 1.6.8 GCP8000 Site Controllers
- 1.6.9 GCM8000 Comparators
- 1.6.10 The Contractor Solutions Logging Interface Equipment
- 1.6.11 PBX switches for Telephone Interconnect
- 1.6.12 NICE and Verint Logging Solutions (if purchased)

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

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

1.9 The Contractor will provide certified hardware version updates and/or replacements necessary to upgrade the system with an equivalent level of functionality up to once in a two-year period. Hardware will be upgraded and/or replaced if required to maintain the existing feature and functionality as per Schedule A Section 4.2. Any updates to hardware versions and/or replacement hardware required to support new features or those not specifically required to maintain existing functionality are not included. Unless otherwise stated, platform migrations such as, but not limited to, stations, consoles, backhaul, civil, network changes and additions, and managed services are not included.

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



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

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

- 1.11.1 GTR 8000 Base Stations
- 1.11.2 GCP 8000 Site Controllers
- 1.11.3 GCM 8000 Comparators
- 1.11.4 MCC 7XXX Dispatch Consoles

1.12 The ASTRO 25 SUA II does not cover all products. Refer to section 3.0 for exclusions and limitations.

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

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

- 1.14.1 Review infrastructure system audit data as needed.
- 1.14.2 Identify additional system equipment needed to implement a system release, if applicable.
- 1.14.3 Complete a proposal defining the system release, equipment requirements, installation plan, and impact to system users.
- 1.14.4 Advise the State of probable impact to system users during the actual field upgrade implementation.
- 1.14.5 Program management support required to perform the certified system upgrade.
- 1.14.6 Field installation labor required to perform the certified system upgrade.
- 1.14.7 Upgrade operations engineering labor required to perform the certified system upgrade.



1.15 ASTRO 25 SUA II pricing is based on the system configuration outlined in Schedule G System Configuration. This configuration is to be reviewed annually from the contract effective date. Pricing may be adjusted, see Schedule A section 4.2.

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

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

2.0 Upgrade Elements and Corresponding Party Responsibilities

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

2.0.1 The Contractor’s responsibilities

2.0.1.1 Obtain and review infrastructure system audit data as needed.

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

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

2.0.1.4 Advise the State of probable impact to system users during the actual field upgrade implementation.

2.0.1.5 Inform the State of high-speed internet connection requirements.

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

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

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

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



- 2.0.2 The State's responsibilities
 - 2.0.2.1 Contact the Contractor to schedule and engage the appropriate The Contractor resources for a system release upgrade.
 - 2.0.2.2 Provide high-speed internet connectivity at the zone core site(s) for use by the Contractor to perform remote upgrades and diagnostics. Specifications for the high-speed connection are provided in Appendix C. High-speed internet connectivity must be provided at least 12 weeks prior to the scheduled upgrade. In the event access to a high-speed connection is unavailable, The State may be billed additional costs to execute the system release upgrade.
 - 2.0.2.3 Assist in site walks of the system during the system audit when necessary.
 - 2.0.2.4 Provide a list of any FRUs and/or spare hardware to be included in the system release upgrade when applicable.
 - 2.0.2.5 Purchase any additional software and hardware necessary to implement optional system release features or system expansions.
 - 2.0.2.6 Provide or purchase labor to implement optional system release features or system expansions.
 - 2.0.2.7 Participate in release impact training at least 12 weeks prior to the scheduled upgrade. This applies only to primary zone core owners. It is the zone core owner's responsibility to contact and include any user agencies that need to be trained or to act as a training agency for those users not included.

- 2.1 System Readiness Checkpoint: All items listed in this section must be completed at least 30 days prior to a scheduled upgrade.
 - 2.1.1 The Contractor's responsibilities
 - 2.1.1.1 Perform appropriate system backups.
 - 2.1.1.2 Work with the State to validate that all system maintenance is current.
 - 2.1.1.3 Work with the State to validate that all available patches and antivirus updates have been updated on the State's system.
 - 2.1.2 The State's responsibilities
 - 2.1.2.1 Validate system maintenance is current.
 - 2.1.2.2 Validate that all available patches and antivirus updates to their system have been completed.

- 2.2 System Upgrade
 - 2.2.1 The Contractor's responsibilities
 - 2.2.1.1 Perform system infrastructure upgrade in accordance with the system elements outlined in this SOW.



2.2.2 The State's responsibilities

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

2.2.2.2 Cooperate with the Contractor and perform all acts that are reasonable or necessary to enable the Contractor to provide software upgrade services.

2.3 Upgrade Completion

2.3.1 The Contractor's responsibilities

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

2.3.1.2 Deliver post upgrade implementation training to the State as needed, up to once per system.

2.3.1.3 Obtain upgrade completion sign off from the State.

2.3.2 The State's Responsibilities

2.3.2.1 Cooperate with the Contractor in efforts to complete any post upgrade punch list items as needed.

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

2.3.2.3 Provide the Contractor with upgrade completion sign off.

3.0 Exclusions and Limitations

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

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

- MCC5500 Dispatch Consoles
- MIP5000 Dispatch Consoles
- Plant/E911 Systems
- MOTOBRIDGE Solutions
- ARC 4000 Systems
- The Contractor Public Sector Applications Software ("PSA")



- Custom SW, CAD, Records Management Software
- Data Radio Devices
- Mobile computing devices such as Laptops
- Non-Motorola two-way radio subscriber products
- Genesis Products
- Point-to-point products such as microwave terminals and association multiplex equipment

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

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

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

4.0 Special provisions

4.1 The State acknowledges that if its System has a Special Product Feature, additional engineering may be required to prevent an installed system release from overwriting the Special Product Feature. Upon request, The Contractor will determine whether a Special Product Feature can be incorporated into a system release and whether additional engineering effort is required. If additional engineering is required, the Contractor will provide to the Program Manager a quote for the change in scope and associated increase in the price for the ASTRO 25 SUA II with back up documentation and mutually agreed upon pricing structure. If acceptable to the State, a change notice incorporating this change will be written by the state and duly executed.

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

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



- 4.4 ASTRO 25 SUA II coverage and the parties’ responsibilities described in this Statement of Work will automatically terminate if the Contractor no longer supports the ASTRO 25 7.x software version in the State’s system or discontinues the ASTRO 25 SUA II program; in either case, the Contractor will refund to The State any prepaid fees for ASTRO 25 SUA II services applicable to the terminated period.
- 4.5 If the State cancels a scheduled upgrade within less than 12 weeks of the scheduled on-site date, The Contractor reserves the right to charge the State a cancellation fee equivalent to the cost of the pre-planning efforts completed by the Contractor Solutions Upgrade Operations Team.
- 4.6 The SUA II annualized price is based on the fulfillment of the ten-year contract. If the State terminates, except if The Contractor is the defaulting party, the State will be required to pay for the balance of payments owed on the most recent two year upgrade, if a system release upgrade has been taken within the past two years prior to the point of termination.

Appendix A – ASTRO 25 System Release Upgrade Paths

ASTRO System Release	Certified Upgrade Paths	
Pre-7.14	Upgrade to Current Shipping Release	
7.14	N/A	7.16 ⁺
7.15	7.16 ⁺	7.17.X*
7.16	N/A	7.18
7.17.X*	N/A	A.2019.1 (Planned)

+ Available upgrade path, but not recommended due to the Software Support Policy

* Includes planned incremental releases

- The information contained herein is provided for information purposes only and is intended only to outline the Contractor’s presently anticipated general technology direction. The information in the roadmap is not a commitment or an obligation to deliver any product, product feature or software functionality and



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

- The most current system release upgrade paths can be found in the most recent SMA bulletin.

Appendix B - System Pricing Configuration

This configuration is to be reviewed annually from the contract effective date. See Schedule G. System configuration. Changes in system configuration may result in a SUA II price adjustment.

Appendix C – High-Speed Connectivity

Specifications Connectivity Requirements

- The minimum supported link between the core and the zone is a full T1
- Any link must realize or a sustained transfer rate of 175 kBps / 1.4 Mbps or better, bidirectional
- Interzone links must be fully operational when present
- Link reliability must satisfy these minimum QoS levels:
 - Port availability must meet or exceed 99.9% (three nines)
 - Round trip network delay must be 100 ms or less between the core and satellite (North America) and 400 ms or less for international links
 - Packet loss shall be no greater than 0.3%
 - Network jitter shall be no greater than 2 ms

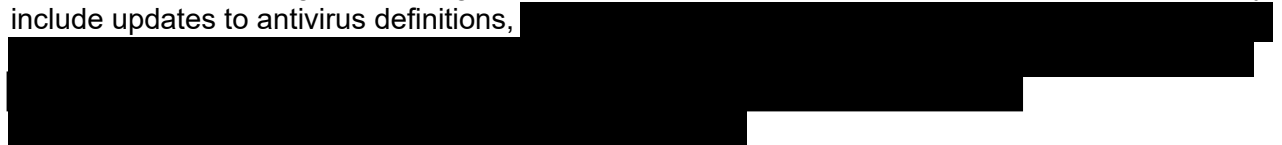


Michigan’s Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

**ATTACHMENT 2 to SCHEDULE A
ASTRO 25 SECURITY UPDATE SERVICE AGREEMENT**

1.0 Description of Security Update Services








The Contractor shall maintain a dedicated vetting lab for each supported ASTRO release for the purpose of pre-testing security updates. In some cases, when appropriate, The Contractor will make the updates available to outside vendors, allow them to test, and then incorporate those results into this offering. Depending on the specific ASTRO release and State options, these may include updates to antivirus definitions,



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

SUS (Self- Installed) is the baseline offer. Sections describing the optional delivery methods and reboot support service are only applicable if purchased.

SUS Delivery Methods

Patch Delivery Method	Download Responsibility	Installation Responsibility	Reboot Support
SUS (Self-Installed)	State	State	*Option 
Remote SUS (Optional)			*Option 
On-Site Delivery of SUS (Optional)			



Packages for L & M Cores

Packaes	SUS (Self Installed)	RSUS	On-Site Delivery of SUS	Reboot Support
Essential / +	✓			Optional
Advanced / +	✓	✓	Optional	Optional
Premier	✓	✓	Optional	Optional

1.1 SUS

Once tested, the Contractor will post the updates to a secured extranet website and send an email notification to the State. If there are any recommended configuration changes, warnings, or workarounds, the Contractor will provide detailed documentation along with the updates on the website. The State will be responsible for the download and deployment of these updates to their ASTRO System.

1.2 Remote Delivery of SUS (RSUS)

Remote Delivery of SUS. The Contractor's dedicated staff remotely installs the required security updates and operating system patches onto your radio network. Vulnerabilities from third party software are addressed as soon as the validation of recommended patches is completed. The Contractor will also provide reports outlining updates made for your team's review and awareness. Patch transfers are transparent to the end user. After the patches are transferred, a report is sent out to inform the State which machines they will need to reboot the appropriate devices to enable the new patches and antivirus definitions.

1.3 Reboot Support Delivery of SUS/RSUS

This optional enhancement provides support for rebooting impacted servers and workstations after the patches have been downloaded/pushed and installed. Once installation is complete, The Contractor will deploy trained technicians to reboot servers and workstations at the State locations.

1.4 ON-SITE Delivery of SUS

For convenience, a trained technician will be contacted to provide the complete patching service. At the State location, the technician will download patches, perform the required installation services and coordinate the rebooting of servers and dispatch ops.

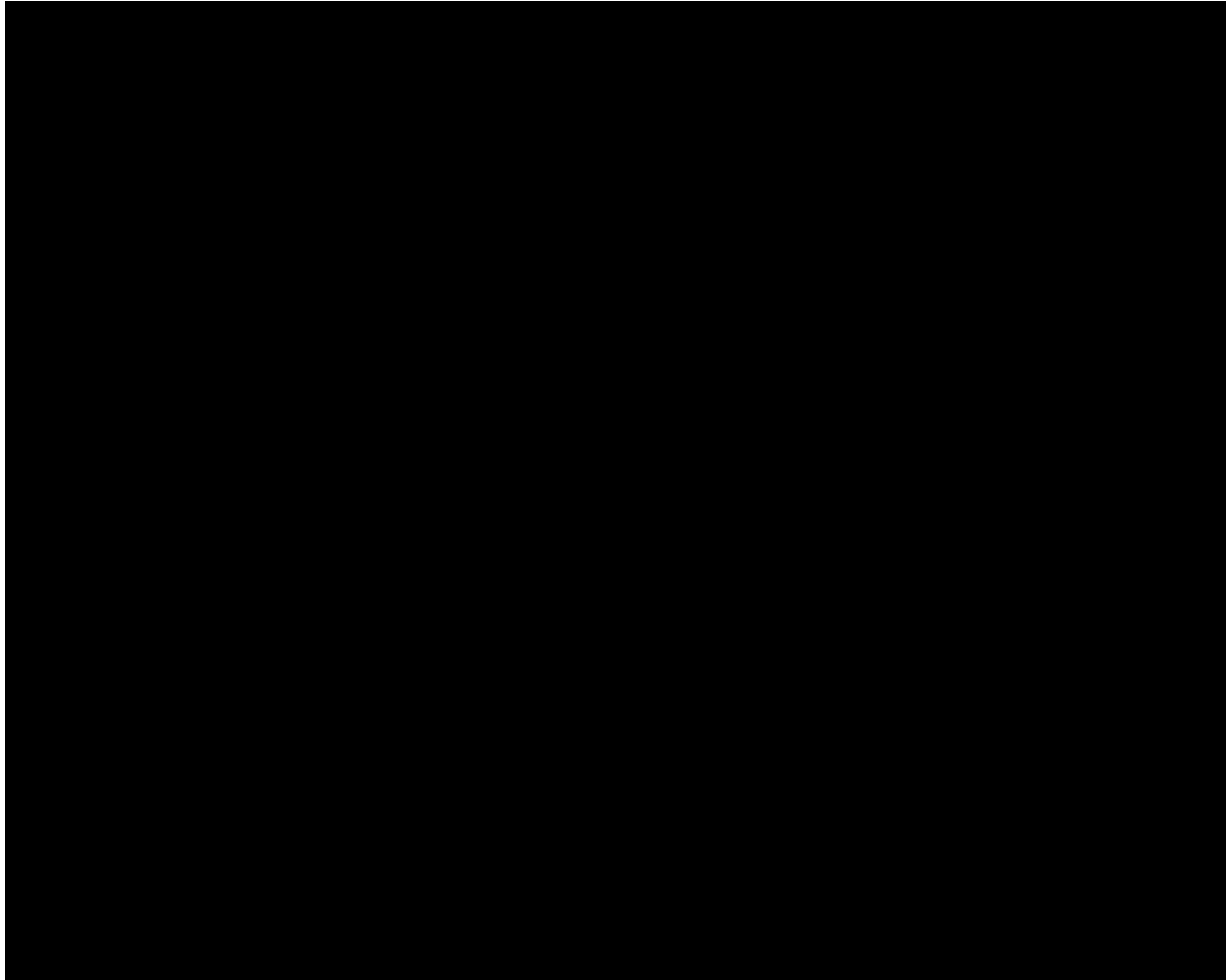
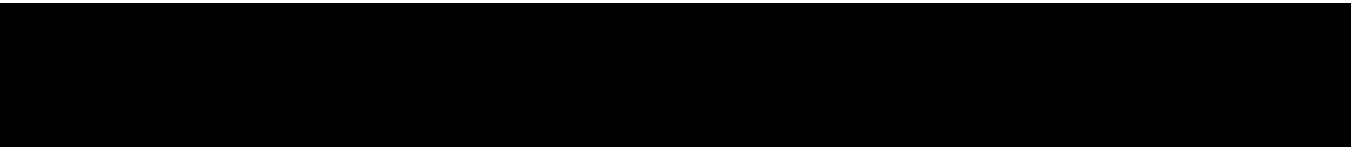
2.0 SUS Scope

- A. Security Update Service supports the currently shipping Motorola ASTRO System Release (SR) and will support 4 releases prior. The Contractor reserves the right to adjust which releases are supported as business conditions dictate.



- B. SUS is available for any L or M core system in a supported release.

- C. Systems that have non-standard configurations that have not been certified by the Contractor Systems Integration and Testing (SIT) are specifically excluded from this Service unless otherwise agreed in writing by the Contractor. Service does not include pre-tested intrusion detection system (IDS) signature updates for IDS solutions as part of SUS/RSUS. However,
 - D. Contractor will make vendor updates available via the secure SUS website. State is responsible for all IDS licensing. Certain consoles, MOTOBRIDGE, MARVLIS, Symbol Equipment, AirDefense Equipment, AVL, and Radio Site Security products are also excluded. The Contractor will determine, in its sole discretion, the third-party software that is supported as a part of this offering.



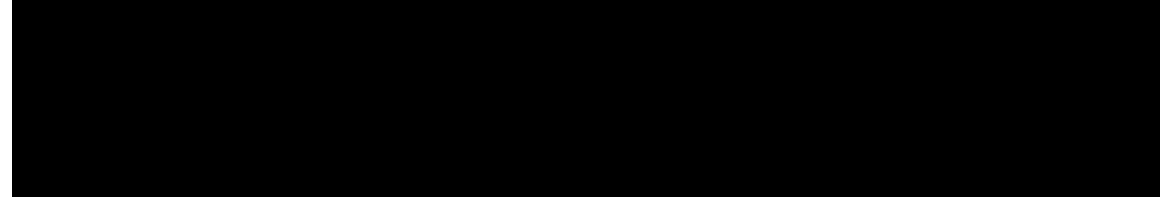


The disk is then prepared, tested and vetted. The disk target release is by the last day of the quarter.

3.0 The Contractor has the following responsibilities:

- A. Obtain relevant 3rd party security updates as made available and supported from the OEM's. This includes antivirus definition, OEM vendor available/supported operating systems patches, [REDACTED]

[REDACTED] The Contractor does not control when these updates are released, but current release schedules are listed for reference:



- B. Each assessment will consist of no less than 36 hours of examination time to evaluate the impact each update has on the system.
- C. Testing of updates to verify whether they degrade or compromise system functionality on a dedicated ASTRO test system with standard supported configurations.
- D. Address any issues identified during testing by working with the Contractor selected commercial supplier and/or the Contractor product development engineering team. If a solution for the identified issues cannot be found, the patch will not be posted on The Contractor's site.
- E. Pre-test STIG recommended remediation when applicable.
- F. Release all tested updates to the Contractor's secure extranet site.
- G. Include documentation for installation, recommended configuration changes, and identified issues and remediation for each update release. H. Include printable labels for States who download the updates to CD's.
- I. Notify State of update releases by email.
- J. A supported SUS ASTRO release matrix will be kept on the extranet site for reference.

4.0 The State has the following responsibilities:

- A. Provide the Contractor with pre-defined information prior to contract start date necessary to complete a State Support Plan (CSP).
- B. Submit changes in any information supplied in the State Support Plan (CSP) to the State Support Manager (CSM).
- C. Provide means for accessing pre-tested files (Access to the extranet website).
- D. Deploy pre-tested files to the State system as instructed in the "Read Me" text provided.



- E. Implement recommended remediation(s) on the State system, as determined necessary by State.
- F. Upgrade system to a supported system release as necessary to continue service.
- G. Adhere closely to the System Support Center (SSC) troubleshooting guidelines provided upon system acquisition. A failure to follow SSC guidelines may cause the State and the Contractor unnecessary or overly burdensome remediation efforts. In such case, the Contractor reserves the right to charge an additional service fee for the remediation effort.
- H. Comply with the terms of the applicable license agreement between the State and the non-Motorola software copyright owner.

5.0 Disclaimer

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



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

ATTACHMENT 3 to SCHEDULE A PremierOne ESSENTIAL MAINTENANCE AND SUPPORT AGREEMENT

PremierOne Maintenance and Support consists of the essential services for Public Safety Applications (PSA) PremierOne Computer Aided Dispatch (P1CAD) and Premier Mobile Data Computer (PMDC) which include Technical and Software Support, and Software Maintenance and related hardware upgrades. The contract will include two (2) hardware upgrade services with replacement and four (4) software upgrades/updates which may be implemented in a timeline of the State's choosing.

1.0 Technical and Software Support

- A. The Contractor will provide technical support and software upgrades for On Demand (OD) and Cumulative Update (CU) releases to apply defect resolutions via phone support and leveraging remote access to the PremierOne system located on the State's network, delivered through a combination of centralized resources within their Technical Support Center (TSC) collaborating with their product development resources. Additionally, the Contractor can provide support via email and via "My View" portal. The Contractor's Responsibilities: 1. Provide availability to the Technical Support Center. See **Section 1.0.B. Severity Level Targets** for all response times:
 - a. 24 hours a day, 7 days a week, every day of the year, to respond to the State's requests for Severity 1 support.
 - b. The Contractor will provide three options to access support services:
 - 1) Via Phone- Contractor's Technical Support Center number is [REDACTED]
 - 2) Via E-mail. See
 - 3) Via the MyView Portal
2. Respond initially to Incidents and Technical Service Requests in accordance with the response times set forth in the Severity Level Response Time Goals section of this document.
3. All calls received will be assigned the impact level in accordance with the Severity Level Response Time Goals
4. Provide caller a plan of action outlining additional requirements, activities or information required to achieve restoration/fulfillment.
5. Maintain communication with the State as needed until resolution of the case.



6. Coordinate technical resolutions with agreed upon third party vendors, as needed.
7. Manage functionally escalated support issues to additional Contractor technical resources, as applicable.
8. Determine, in its sole discretion, when a case requires more than the Technical Support services described and notify the State of an alternative course of action.

B. Severity Level Targets

1. Response Time Goals

The Contractor will meet the technical support response time goals set forth in the table below:

RESPONSE TIME GOAL		
Severity Level	Description	Response Time
Severity 1	<p>Total System Failure - occurs when the System is not functioning and there is no workaround; such as a Central Server is down or when the workflow of an entire agency is not functioning. This level is meant to represent a major issue that results in an unusable System, Subsystem, Product, or critical features. No work around or immediate solution is available.</p> <p>A Contractor TSC Technician will respond within one hour of the request for support being logged in the issue management system. Continual effort will be maintained to restore the system or provide a workaround resolution. Response provided 24 x 7.</p>	Telephone conference within 1 Hour of initial verbal notification , Continuously.
Severity 2	<p>Non-Critical Major Failure - This error level occurs when a major but noncritical element in the System is not functioning but that does not prohibit continuance of basic operations. There is usually no suitable workaround. Note that this may not be applicable to intermittent problems. This level is meant to represent a moderate issue that limits a The State's normal use of the System, Subsystem, Product or major non-critical features.</p>	Telephone conference within 3 Business Hours of initial verbal notification during normal (standard) business hours. Standard Business Day - Monday through Friday 8AM to 5PM, ET, excluding US Holidays.
Severity 3	<p>Non-Critical Minor Failure- Non-Critical part or component failure occurs when a System component is not functioning, but the System is still useable for its intended purpose, or there is a reasonable workaround. This level is meant to represent a minor issue that does not preclude use of the System, Subsystem, Product, or critical features.</p>	Telephone conference within 8 Business Hours of initial notification during normal (standard) business hours. Standard Business Day- Monday through Friday 8AM to 5PM, excluding US Holidays.



RESPONSE TIME GOAL		
Severity Level	Description	Response Time
Severity 4	<p>Non-Critical Minor Failure- Non-Critical part or component failure occurs when a System component is not functioning, but the System is still useable for its intended purpose, or there is a reasonable workaround. This level is meant to represent a minor issue that does not preclude use of the System, Subsystem, Product, or critical features.</p> <p>Minor issues include but are not limited to: cosmetic issues, documentation errors, general usage questions, and product or System Update requests.</p>	<p>Telephone conference within two (2) Standard Business Days of initial notification. Standard Business Day - Monday through Friday 8AM to 5PM, excluding US Holidays.</p>

2. Severity Level Escalation

- a. Once an issue is escalated to Engineering, the following table is used as an Engineering resolution guideline for standard product problems.

Escalation Policy- Severity Level 1		
CRITICAL	ACTION	RESPONSIBILITY
0 Hours	Initial service request is placed. Support Analyst begins working on problem and verifies / determines severity level.	Support Analyst
2 Hours	If a resolution is not identified within this timeframe, SA escalates to the Customer Support Manager who assigns additional resources. Email notification to Director of Customer Support and Director of System Integration.	Support Analyst Support Manager
4 Hours	If a resolution is not identified within this timeframe, Customer Support Manager escalates to the Director of Customer Support and Director of System Integration to assign additional resources. Email notification to Vice President of System Integration and Vice President Customer Support.	Support Manager Director of Customer Support Director of Systems Integration
8 Hours	If a resolution is not identified within this timeframe, Director of Customer Support escalates to Vice President of System Integration, Vice President of Support, and Account Team.	Support Manager Director of Customer Support Director of Systems Integration VP of System Integration VP of Customer Support
12 Hours	If a resolution is not identified within this timeframe, Director of Customer Support escalates to Vice President of System Integration, Vice President of Support, and Account Team, Senior Vice Presidents of Operations, System Integration, Customer Support and Engineering.	Senior Management Support Operations Systems Integration Engineering



- b. All Severity Level 1 problems will be transferred or dispatched immediately to the assigned Contractor technical support representative, to include notification to Contractor management 24x7. All other severity level problems logged after business hours will be dispatched the next business morning.

C. Accessing Customer Support

1. Option 1- Toll-Free call to Contractor Technical Support Center for support and updates at [REDACTED].

- a. Select phone option 4 for Contractor's Public Safety Applications, then option 2 for support related to Computer-aided Dispatch and Mobile. From there selection option 2 for PremierOne Legacy CAD/Mobile
- b. Select phone option 4 for support related to Records / Jail Management. From there select option 2 for PremierOne, Legacy Records
- c. Upon contact with the SSC/TSO personnel, the caller will provide the name and phone number for the State contact and your agency and Site ID [REDACTED]. [REDACTED] Providing a brief problem description will assist in defining the severity level and determine proper case routing to the appropriate Contractor Technical Support Team Member. A unique tracking number will be provided to your agency for future reference.
- d. Generally, the State calling the toll-free 800 number will access Applications Technical Support directly. For heavy call times or after hours the caller will be directed to Contractor System Support Call Center Operations. Once the logging process is complete the State transferred directly to a Technical Support Analyst 24/7/365.

2. Option 2- Submit a ticket via Email Case Management for Security Levels (3) three and (4) four only.

The State can request technical support by email. For many customers who use their PDA as a means to open cases, email ticketing provides additional flexibility for initiating cases. To properly process a ticket, the message must be formatted exactly as described below:

- a. **Address Email to:** [REDACTED]
- b. **Subject:** Type PSA Service Request and Brief Description of the problem (This becomes the case title)
- c. **Body of the Email:** Use the following template for the body of the email. You can copy and paste from below, filling in the accurate and specific needs of the request following the bold items listed:



- 2) **Product Type** = followed by the product family type. Choose from the following list:

- 3) **Contact First Name** = followed by your first name or the name of the person you would like support personnel to contact
- 4) **Contact Last Name** = followed by your last name or the name of the person you would like support personnel to contact.
- 5) **Phone Number** = followed by the area code and phone number where the contact person may be reached
- 6) **Severity Level** = followed by either severity level 3 or 4. All severity level one or two cases must be opened via the tollfree customer support number
- 7) **Problem Description** = followed by a comprehensive description of the problem
- 8) **Send the message to the Contractor.** You will receive an email with your case number for future reference

- d. **IMPORTANT NOTE:** Please note that use of certain special characters, html signatures, or the inclusion of certain attachment types may cause the originating email to be blocked by the Contractor's Proofpoint Protection Server as per Contractor security policy. See the list of blocked attachments below:

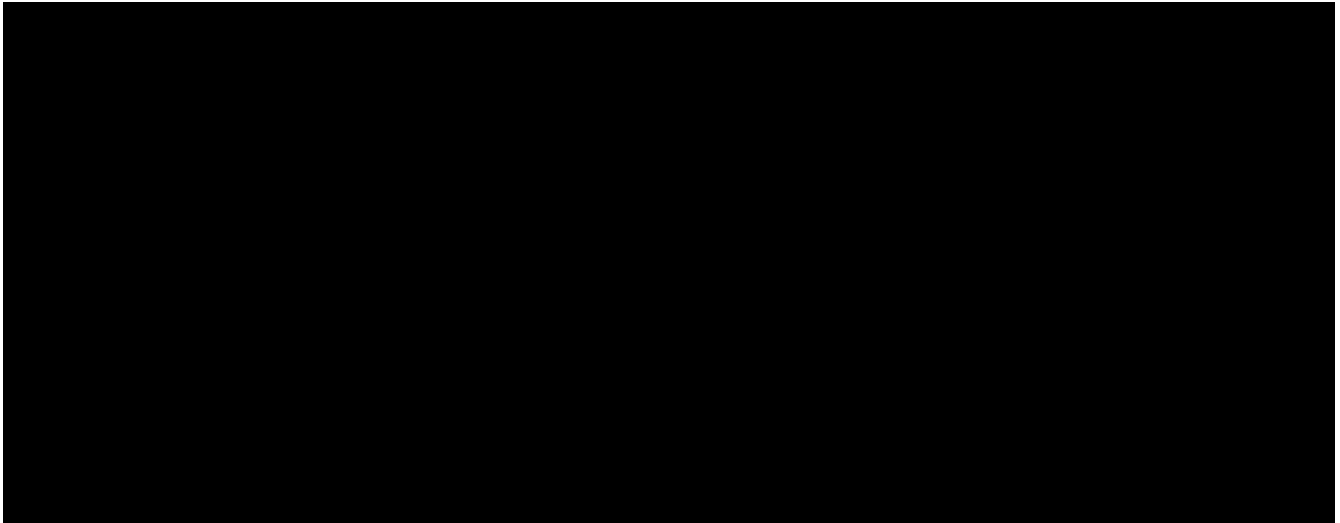
"ade" or "adp" or "ani" or "bas" or "bat" or "chm" or "cmd" or "com" or "cpl" or "crt" or "exe" or "hlp" or "ht" or "hta" or "inf" or "ins" or "isp" or "job" or "js" or "jse" or "lnk" or "mda" or "mdb" or "mde" or "mdz" or "msc" or "msi" or "msp" or "mst" or "pcd" or "pif" or "reg" or "rtf" or "scr" or "sct" or "shs" or "url" or "vb" or "vbe" or "vbs" or "wsc" or "wsf" or "wsh" or "wmf" or "386" or "3gr" or "add" or "asp" or "dbx" or "dll" or "fon" or "ocx" or "shb" or "vxd" or "lib" or "sys"

- e. If an email response including the new case number is not received, or if you need to open a severity level one or two case,



please contact the Contractor's Customer Support at [REDACTED]
[REDACTED] for further assistance.

f. Sample Ticket Formatting:



3. Option 3- Case Management via MyView Portal.

MyView Portal provides actionable insights into your mission-critical operations, giving you the knowledge to make data-driven decisions that mitigate the risk of downtime and enhance system performance. With Essential Service Package, MyView Portal gives you valuable system and service information whenever you need it along with complete support case/incident management from submission to close.

D. Security

The Contractor will maintain industry standard security measures to protect the Solution from intrusion, breach, corruption, or other security risk.

1. During the term of the Agreement, if the Solution enables access to Criminal Justice Information (CJI), as defined by the most recent Federal Bureau of Investigations Criminal Justice Information Services Security Policy (CJIS) and the Michigan Administrative Rules, The Contractor will provide and comply with the most recent FBI CJIS Security and the Michigan Security Addendum. Any additional Security measure desired by the State may be available for an additional fee.
2. The Contractor will require its personnel that have unescorted access to unencrypted CJI or unescorted access to configure and maintain computer systems and networks with direct access to CJI to undergo a state of residency and national fingerprint-based background check and a namebased check.
 - a. The background check will be administered by the State.



- b. These personnel will also be required to complete the appropriate level of CJIS specific Security Awareness Training within six (6) months of assignment and thereafter every two (2) years. The Contractor will provide proof of completion to the State.
 - c. Each person must also sign the FBI CJIS Security Addendum and provide a copy to the State.
 3. The FBI CJIS Security Addendum, appended, is incorporated by reference and made a part thereof as if fully appearing in Schedule A – Attachment 7.
 4. The State is independently responsible for establishing and maintaining its own policies and procedures and for ensuring compliance with FBI CJIS Security Policy, the Michigan Security Addendum and other security requirements that are outside the scope of the Service provided.
 5. The State will establish and ensure compliance with access control policies and procedures, including password security measures.
 6. The State will maintain industry standard security and protective data privacy measures.
 7. Contractor Disclaimers:
 - e. The Contractor disclaims any responsibility or liability whatsoever for the security or preservation of Customer Data or Solution Data once accessed or viewed by the State or its representatives.
 - f. The Contractor disclaims any responsibility or liability whatsoever for the State's failure to maintain industry standard security and data privacy measures and controls, including but not limited to lost or stolen passwords.
 - g. The Contractor reserves the right to terminate the Service if the State's failure to maintain or comply with industry standard security and control measures negatively impacts the Service, Solution, or Contractor's own security measures.

E. Service Offerings

1. The Contractor's customer support organization will include a staff of Support Analysts who are managed by Contractor Customer Support managers and are chartered with the direct front-line support for the State.
2. A Support Analyst is a system technologist responsible for providing direct or escalation support. A Support Analyst is sometimes referred to as a Customer Support Analyst ("CSA") or Technical Support Analyst ("TSA") or Technical Support Representative.
3. Contractor's Levels of support are defined as follows:



Level 0	Logging, dispatching and tracking service requests
Level 1	Selected 1 st call support, triage and resolution
Level 2	Telephone and/or on-site support for normal technical requirements
Level 3	High-level technical support prior to Engineering escalation
Level 4	Engineering software code fixes and changes

4. Contactor’s Technical Support Contacts

In addition to the toll-free number the following staff members are available for escalation:

CONTACT	PHONE NUMBER
Contractor Solutions System Support Center	[REDACTED]
Dave Wojtylko Customer Support Manager [REDACTED]	[REDACTED]
Phillip Askey Technical Support Manager – Command & Control (PSA) Applications [REDACTED]	[REDACTED]
Brian Bullock Account Executive, Manager [REDACTED]	[REDACTED]

F. Limitations and Exclusions

The following activities are outside the scope of the Technical Support service, but are available to remote Technical Support customers, such as the State, at an additional cost, which will be quoted for consideration at the State’s request:

1. On-site visits /resources
2. System installations, upgrades, and expansions
3. Hardware replacement/exchange
4. Contractor implementation or on-site upgrade services



5. Proactive Solution Monitoring

G. The State's Responsibilities:

1. Contact the Contractor's Technical Support Center in order to engage the Technical Support service, providing the necessary information for proper entitlement services. Including but not limited to:
 - a. the name of contact/name of the State,
 - b. system ID number,
 - c. site(s) in question, and
 - d. brief description of the problem including pertinent information for initial issue characterization.
2. Maintain suitable trained technical resources that provide technical maintenance services to the system, and who are familiar with the operation of that system.
3. Supply suitably skilled and trained on-site presence when requested by the TSC.
4. Send validation to the Contractor within 24 hours of issue resolution prior so that the case may be closed in a timely manner.
5. Cooperate with the Contractor and perform all acts that are reasonable or necessary to enable the Contractor to provide the Technical Support.
6. If necessary, obtain at the State's cost all third-party consents or licenses required to enable the Contractor to provide the service.
7. Monitor SCOM alerts and notify TSC of any issues requiring technical resolution.

2.0 Software Upgrades and Maintenance

As new PremierOne releases become available, the Contractor will provide the State with the software required to execute an upgrade for their PremierOne system. Remote upgrade services are included for On Demand (OD) and Cumulative Upgrade (CU) releases that may be available. Standard Release (SR)

installation labor services are not included. Software releases include any Contractor software updates that may be available. The Contractor will only provide releases that have been analyzed, pre-tested, and certified in a dedicated PremierOne test lab to ensure application functionality.



A. Definitions

1. “Releases” means an Update or Upgrade to the Contractor Software and are characterized as “On Demand Releases,” “Cumulative Updates,” “Supplemental Releases,” “Standard Releases,” or “Product Releases.” The content and timing of Releases will be at the Contractor’s sole discretion.
2. A “Cumulative Update” is defined as a release of Contractor Software that contains error corrections to an existing Standard Release that do not affect the overall structure of the Contractor Software. Cumulative Updates will be superseded by the next issued Cumulative Update.
3. A “Supplemental Release” is defined as an interim release of Contractor Software that contains primarily error corrections to an existing Standard Release and may contain limited improvements that do not affect the overall structure of the Contractor Software. Depending on the State’s specific configuration, a Supplemental Release might not be applicable.
4. A “Standard Release” is defined as a release of Contractor Software that may contain product enhancements and improvements, such as new databases, modifications to databases, or new servers, as well as error corrections. A Standard Release may involve file and database conversions, System configuration changes, hardware changes, additional training, on-site installation, and System downtime. Standard Releases will contain all the content of prior On Demand Releases and Cumulative Updates that is reasonably available (content may not be reasonably available because of the proximity to the end of the release cycle and such content will be included in the next release).
5. A “Product Release” is defined as a release of Contractor Software considered to be the next generation of an existing product or a new product offering. If a question arises as to whether a Product offering is a Standard Release or a Product Release, Contractor’s opinion will prevail, provided that Contractor treats the Product offering as a new Product or feature for its end user customers generally.
6. On Demand Releases are identified by the fifth character of the fivecharacter release number, shown here as underlined: “1.2.0.4.a,” Cumulative Updates by the fourth digit: “1.2.0.4.a,” Supplemental Releases are identified by the third digit: “1.2.0.4.a,” Standard Releases by the second digit: “1.2.0.4.a,” and Product Releases by the first digit: “1.2.0.4.a.”

**B. Scope:**

1. The PremierOne certified release software. Other products are not included. See subsection **2.1.B. Limitations and Exclusions**.
2. Software Maintenance applies only to software release upgrades within the previous two releases from the current PremierOne version.
3. Contractor Response. Contractor will provide telephone and on-site response to Central Site, defined as the State's primary data processing facility, and Remote Site, defined as any site outside the Central Site on the PremierOne CAD and PremierMDC as part of this Agreement.
4. Remote Installation. At the State's request the contractor will provide remote installation advice or assistance for updates.
5. On-Site Software Correction. All support will be investigated and corrected from the Contractor's facilities. The Contractor will make the determination whether on-site correction of any residual error is required and will take appropriate action.
6. Reports. Service history reports and notifications will be available, upon the State's request, from the Contractor call tracking system.
 - a. To obtain access to service history reports and ticketing notifications will request them from the Contractor's Technical Support Representative.
7. Compliance with Local, County, State and/or Federal Mandated Changes. (Applies to Software and interfaces to those Products).
 - a. Compliance to local, county, state and/or federally mandated changes, including but not limited to NCIC and state interfaces are not part of the covered Services.
 - b. Federal and State mandated changes for IBR and UCR are included in Contractor's standard maintenance offering.
8. The State agrees to:
 - a. Contact the Contractor to schedule and engage the appropriate Contractor resources to obtain resources for a PremierOne release upgrade.
 - b. Purchase or provide any labor needed to implement system release upgrades.
 - c. Purchase any additional hardware and software needed to implement any optional solution features or number of users/new service expansions.



- d. Provide or purchase labor to implement optional solution features or number of licenses/new service expansions.
- e. Cooperate with the Contractor and perform all acts that are reasonable or necessary to enable Contractor to provide software upgrade services. **C. Limitations and Exclusions:**
 - 1. Non-Standard configurations that have not been certified by Contractor Systems Integrations Testing are specifically excluded from the PremierOne SMA unless otherwise agreed in writing via Change Notice by the Contractor and the State.
 - 2. The PremierOne Software Maintenance does not include the following:
 - a. Contractor networks and infrastructure products
 - b. Non- Motorola network and infrastructure products
 - c. Contractor Command Central Software
 - d. Custom software or third-party application software
 - e. Data radio devices
 - f. Mobile computing devices such as laptops
 - g. Motorola and Non-Motorola two-way radio subscriber products
 - h. Point-to-point products such as fiber, LAN/WAN, microwave terminals and association multiplex equipment
 - i. PremierOne SMA does not cover any hardware or software supplied by or to the State when purchased directly from a third party, unless specifically included or added via Change Notice.
 - j. PremierOne SMA does not cover software support for virus attacks or other applications that are not part of the PremierOne system, or unauthorized modifications or other misuse of the covered software. Contractor is not responsible for management of antivirus or other security applications.
 - k. Upgrades for equipment add-ons or expansions during the term of this PremierOne unless specifically included or added via Change Notice.

D. Special Provisions:

- 1. The State will only use the software (including any System Releases) in accordance with the applicable Software License Agreement.



2. PremierOne SMA services do not include repair or replacement of hardware or software that is necessary due to defects that are not corrected by the system release, nor does it include repair or replacement of defects resulting from any nonstandard, improper use or conditions; or from unauthorized installation of software.
3. PremierOne SMA coverage and the parties' responsibilities described herein will automatically terminate if the Contractor no longer supports the PremierOne software version in the State's system or discontinues the PremierOne SMA program; in either case, The Contractor will refund to the State any prepaid fees for PremierOne Software Maintenance services applicable to the terminated period.
4. If the State cancels a scheduled upgrade within less than 12 weeks of the scheduled-on site date, the Contractor reserves the right to charge the State a cancellation fee equivalent to the cost of the pre-planning efforts completed by the Contractor Upgrade Operations Team.
5. The Software Maintenance annualized price is based on the fulfillment of the 12-month term. If the State terminates, except if Contractor is the defaulting party, the State will be required to pay for the balance of payments owed if a system release upgrade has been taken prior to the point of termination.

E. The State's Responsibilities:

1. Troubleshooting. The State will make every effort to triage issues internally. If Contractor assistance is requested, the State will make all reasonable efforts to assist in problem resolution. This may include problem reproduction, answering questions, supplying data, etc.
2. Initiate Service Request Cases. Contact Contractor through authorized tools and processes outlined in **Section 1.0.C** to initiate technical support request case.
3. Assess Severity Level. Assist in assessing and assigning the initial and the correct severity level per the severity level definitions found in **Section 1.0.B**.
4. Escalate Appropriately. Contact the Contractor to add information or make changes to existing technical support cases or to escalate service requests to Contractor management.
5. Maintenance on Hardware. The State will provide all on-site hardware maintenance and service or is responsible for purchasing on-going maintenance for 3rd party on-site hardware support unless third-party support is already contracted with the Contractor.



- a. The State will contact the appropriate vendor directly for parts and hardware service, if not purchased through the Contractor.
6. VPN connectivity. Provide VPN connectivity and telephone access to Contractor personnel.
7. Operating System (“OS”) Upgrades. The State is responsible for any OS upgrades to the System, except HP OS upgrades. Before installing OS upgrades, the State will contact the Contractor to verify that a given OS upgrade is appropriate and will not adversely impact the system.
8. SCOM Monitoring. Monitor system for notifications sent by SCOM, resolve related issues and/or contact the Contractor to open a case for technical support assistance.
9. Physical and Virtual Server Maintenance. Apply upgrades such as OS patches, administrative tools and utilities. Maintain and upgrade software that supports infrastructure applications. Perform periodic reboots and ongoing performance tuning, hardware upgrades, and resource optimizations as required.
10. Event Log Review. Review System and Application Event Logs periodically to identify any possible problems, and/or unrecognized or frequent errors.
11. Physical Workstation Maintenance. Perform periodic reboots and ongoing performance tuning, hardware upgrades, and resource optimizations as required. Inspect physical equipment for damage or wear, replace parts as per contractual agreement.
12. CAD Client Maintenance. Apply upgrades such as OS patches, administrative tools and utilities. Maintain and upgrade software that supports infrastructure applications (IE, Esri, etc.). Perform periodic reboots and ongoing performance tuning, hardware upgrades, and resource optimizations as required. Upgrade and maintain antivirus software, appropriately configure and maintain exclusion list.
13. Mobile Client Maintenance. Apply upgrades such as OS patches, administrative tools and utilities. Maintain and upgrade software that supports infrastructure applications (IE, Esri, etc.). Perform periodic reboots and ongoing performance tuning, hardware upgrades, and resource optimizations as required. Upgrade and maintain antivirus software, appropriately configure and maintain exclusion list. Configure and maintain all products relevant to mobile network connectivity (NetMotion, Verizon, VPN related products, etc.).
14. Third-Party Maintenance:



- a. .Net. Install, upgrade, configure, and maintain .net framework software as per minimum requirements outlined by the Contractor.
 - b. Server. Install, upgrade, configure, and maintain all servers hosting 3rd party products that interface to Contractor products. See Physical Server Maintenance section above for additional explanation.
 - c. SQL. Install, upgrade, configure, and maintain MSSQL application. Make resource optimization changes pertaining to best practices as required by the Contractor.
 - d. SQL Express. Install, upgrade, configure, and maintain MSSQL Express application. Make resource optimization changes pertaining to best practices as required by the Contractor.
 - e. Unembedded Third-Party Licensing. Maintain and apply all thirdparty licensing for products not specifically embedded within an Contractor proprietary product.
15. DB Failover (Post 4.0). Perform and periodically test system database failover via script or MSSQL tools.
- a. Engage Contractor's Support and provide supporting data for any problems discovered. Perform and periodically test system disaster recovery site failover via script provided by the Contractor.
 - b. Officially notify the Contractor of any plans to perform DR failover with reasonable advance notice.
 - c. Engage Contractor Support and provide supporting data for any problems discovered.
16. Data Purging. Perform regular file archival and purge as necessary. Configure data purges compliant with government mandates and internal retention protocols. Maintain adequate storage space to ensure that retention of required data will not adversely impact the MPSCS and Contractor Systems.
17. Storage Capacity Tracking and Maintenance. Monitor, maintain, and configure system data storage components in accordance with accepted standards and operational requirements as outlined by Contractor. Act on any storage related SCOM notification in accordance with the SCOM monitoring standards outlined above.
18. Temporary DB File Size Maintenance. Monitor system temporary database size and available storage. Act on any related SCOM notifications in accordance with the SCOM monitoring standards outlined above.
19. RDW Maintenance. See Physical/Virtual Server above.



20. Customer Reports. Build/Modify/Support all custom reports in a manner that will not adversely impact RDW Server/Database functionality. Custom reports are the sole responsibility of the creator and not supported by the Contractor.
21. CAD/Mobile Client Install and Testing. Install, upgrade, and test P1 Software Updates (includes Standard, CU and ODs). Report and supply data for any problems that are discovered with the software to the Contractor for review and correction. Ensure that minimum software/hardware requirements are met.
22. GIS Updates - PremierOne Map Maintenance.
 - a. Ensure validity and integrity of all GIS related data introduced to the system.
 - b. Record modifications made to GIS files, and confirm expected behavior within the PremierOne system.
 - c. Perform all server mapping updates, geoset transitions, and distribute updated map files to CAD/Mobile clients.
24. Anti-Virus and Windows UAC. Install, configure, and upgrade chosen anti-virus software.
 - a. Appropriately configure user account control settings in a manner that ensures the files are accessible for system stability and successful operation.
 - b. If system instability occurs after changing any system element pertaining to UAC or AV, report changes to the Contractor.
 - c. If unexpected behavior is experienced while UAC or AV are enabled, and does not occur after disabling UAC or AV, the State will be responsible for diagnosing and correcting the issue.
 - d. Per the State's request, the Contractor will make every reasonable effort to test and verify specific anti-virus patches against a replication of the State's application if a problem cannot be resolved internally.
25. System, Database, HD and Tape Backups. Perform and/or ensure successful completion of daily backup operations.
 - a. Ensure that all required system files and data are successfully backed up to the appropriate media.
 - b. Monitor health of all backup related hardware, including but not limited to HP tape library, recovery tapes, and disk drives.



- c. Maintain and upgrade backup related software, such as HP DataProtector.
 - d. Prior to performing system or database upgrades, create a backup of the system and/or database to maintain a restoration point.
 - e. Ensure that PremierOne SSMS full and incremental database backups completing successfully, report related SCOM notifications to the Contractor.
26. Provisioning knowledge of the system. The State must ensure that adequate provisioning training and knowledge has been provided to those authorized to access and/or make changes within PremierOne Provisioning.
- a. Provisioning changes should be tracked.
 - b. This information should be supplied to the Contractor to aid in troubleshooting efforts should a problem be experienced.
 - c. The Contractor provides a tool to aid in provisioning change identification, but changes should be tracked internally by the State as a failsafe.
27. Records ACT. Only trained users of ACT should attempt to use ACT to maintain their system.
- a. New module creation, or existing module changes, should first be completed and tested within a non-production environment.
 - b. Apply changes to the production environment by running a build-set or importing the ash file(s).
 - c. All changes made in ACT should be tracked via the Contractor's supplied excel files.
 - d. These files must be made available upon request to aid in the Contractor's troubleshooting efforts.
 - e. ACT additions, changes, and maintenance is the sole responsibility of the State.
28. Use of Deployment or All-In-One. Users of the deployment tool or AIO tool must be appropriately trained and understand its operation fully.
- a. Deployment packages that are no longer necessary should be purged.
 - b. The State is responsible for client deployment and should engage Contractor support if a problem is discovered.



29. Tape and HD Backup Rotation. See Backup.
30. Gathering Issue Logs (Server and Client). Supply all requested logs for problems that need to be diagnosed and resolved. In some circumstances, log automation will be implemented, however anything that is not automatically gathered, and deemed necessary by the Contractor, must be furnished. Absence of requested data may lead to case closure.
31. Data Archiving. The State is responsible for all P1 Data Archival as per their internal requirements and needs. Adequate storage space should be maintained, and data must not be stored in a manner that adversely impacts the PremierOne System or component operations.
32. Network Bandwidth and Stability. Install, monitor, and maintain network systems that provide stable operations and adhere to bandwidth requirements to ensure the effective operation of the Contractor's products and related system components.
33. Remote Access. Upon successful completion of approved background check, the State will provide remote access to requesting Contractor personnel for troubleshooting purposes. This includes, but is not limited to, VPN account access, remote hosting, PremierOne domain access, and access to all system elements that pertain to the operation of the PremierOne CAD system and functionality.
34. User Access Control. See Anti-Virus.
35. Backup Power. Install and maintain backup power source to ensure the effective operation of the PremierOne CAD System and all its components in the event of a primary power source failure.
36. End User Training. Ensure that all end users of the Contractor's products are adequately trained to perform their duties and not cause harm or upset of system functionality. The Contractor will offer additional training, if the State deems necessary, for an additional cost.
37. Change Management. Notify the Contractor of any changes made to the PremierOne CAD System, associated interfaces, related hardware, software, network, or any other system element that may adversely impact operation or system functionality.

3.0 Scope and Term of Services

- A. If the price for Services is based upon a per unit fee, such price will be calculated on the total number of units of the Products that are licensed to the State as of the beginning of the maintenance and support period. If, during a maintenance and support period, the State acquires additional Products that will be covered by this Agreement, the price for maintenance and support services for the additional Products will be calculated and



added to the total price either (1) if and when the maintenance and support period is renewed or (2) immediately when the State acquires additional Products, as determined by Contractor. Contractor may adjust the price of the maintenance and support services at the time of a renewal if it provides to State notice of the price adjustment at least forty-five (45) days before the expiration of the maintenance and support period. If the State notifies Contractor of its intention not to renew this Agreement as permitted by Section 3.2 and later wishes to reinstate this Agreement, it may do so with the State's consent provided (a) the State pays to the Contractor the amount that it would have paid if the State had kept this Agreement current, and (b) the State ensures that all applicable Equipment is in good operating conditions at the time of reinstatement.

- B. When Contractor performs Services at the location of installed Products, the State agrees to provide to the Contractor, at no charge, a nonhazardous environment for work with shelter, heat, light, and power, and with full and free access to the covered Products. The State will provide all information pertaining to the hardware and software with which the Products are interfacing to enable the Contractor to perform its obligations under this Agreement.
- C. All the State requests for covered Services will be made initially with the call intake center.
- D. Contractor will provide to the State Technical Support Services and Releases as follows:
 - 1. Contractor will provide Technical Support Services and correction of Residual Errors during the PPM in accordance with the Exhibits. Any Technical Support Services that are performed by Contractor outside the contracted PPM and any Residual Error corrections that are outside the scope will be billed at the then current hourly rates. The objective of Technical Support Services will be to investigate specifics about the functioning of covered Products and to determine whether there is a defect in the Product. Technical Support Services will not be used in lieu of training on the covered Products.
 - 2. Contractor will provide to the State without additional license fees an available Cumulative Update, Supplemental, or Standard Release for the Contractor's PremierOne Applications after receipt of a request from the State. The State must pay for any installation or other services and any necessary Equipment or third party software or training provided by Contractor in connection with Supplemental or Standard Releases. On Demands and Cumulative Updates are designed to be delivered remotely. Services for onsite delivery related to On Demands and Cumulative Updates as requested by the State will be quoted at the time



of the request. Any services will be performed in accordance with a mutually agreed schedule.

3. The Contractor will provide to the State an available Product Release after receipt of a request from the State, but the State must pay for all additional license fees, any installation or other services, and any necessary Equipment provided by the Contractor in connection with such Product Release. The Contractor's duty as described in this paragraph is contingent upon the State's then-current installation at the time of the State's request being within two (2) Standard Release versions of the new Standard Release available for general release. Any services will be performed in accordance with a mutually agreed schedule.
4. Along with maintenance Software Releases, the Contractor will make available new purchasable products, features and modules which are separate and distinct from the mainstream PremierOne line of Products. Newly released Products may have PremierOne as a pre-requisite and/or share some portion of the PremierOne code base. The State is not entitled to these products, features and modules, or upgrades to them within this Maintenance and Support Agreement, if they have not purchased the required licenses.
5. As part of the Software development process the Contractor makes every reasonable effort to lessen impact to the State operations. Any change to existing functionality is done after thorough review of the State feedback and with announcement of said change. When it's not technically feasible to meet a particular requirement the Contractor will proactively communicate the changes. Beyond these efforts Contractor does not warrant that a Release will meet the State's particular requirement, be uninterrupted or error-free, be backward compatible, or that all errors will be corrected. Errors addressed as part of the Software Release will be corrected. Full compatibility of a Release with the capabilities and functions of earlier versions of the Software may not be technically feasible. If it is technically feasible, the Contractor will make available services to integrate these capabilities and functions to the updated or upgraded version of the Software, which services may be fee based.
6. The Contractor's responsibilities under this Agreement to provide Technical Support Services in accordance with the package selected by the State and as further detailed in the statement of work, customer support plan will be limited to the current Standard Release plus the two (2) prior Standard Releases (collectively referred to in this section as "Covered Standard Releases"). Notwithstanding the preceding sentence, the Contractor will provide Technical Support Services for a Severity Level 1 or 2 error concerning a Standard Release that precedes the Covered Standard Releases unless such error has been corrected by a



Covered Standard Release (in which case the State will need to have the Standard Release that fixes the reported error installed or terminate this Agreement as to the applicable Software).

7. The Contractor's responsibilities under this Agreement to provide Technical Support Services will be limited to the current Standard Release concerning the following Software: Customer Service Request, Case Management, Integration Framework, and Integration Framework Express.

E. The maintenance and support Services described in this Agreement are the only covered services. Unless Optional Technical Support Services are purchased, these Services specifically exclude and Contractor will not be responsible for:

1. Any service work required due to incorrect or faulty operational conditions, including but not limited to Equipment not connected directly to an electric surge protector, or not properly maintained in accordance with the manufacturer's guidelines. Other services may be available for an additional fee and will be addressed with an amendment to the Agreement.
2. The repair or replacement of Products or parts resulting from failure of the State's facilities, State's personal property and/or devices connected to the System (or interconnected to devices) whether or not installed by the State's representatives.
3. The repair or replacement of Equipment that has become defective or damaged due to physical or chemical misuse or abuse, the State's negligence, or from causes such as lightning, power surges, or liquids.
4. Any transmission medium, such as telephone lines, computer networks, or the worldwide web, or for Equipment malfunction caused by such transmission medium.
5. Accessories, custom or Special Products; modified units; or modified Software.
6. The repair or replacement of parts resulting from the tampering by persons unauthorized by the Contractor or the failure of the System due to extraordinary uses.
7. Operation and/or functionality of the State's personal property, equipment, and/or peripherals and any application software not provided by Contractor.



8. Services for any replacement of Products or parts directly related to the removal, relocation, or reinstallation of the System or any System component.
9. Services to diagnose technical issues caused by the installation of unauthorized components or misuse of the System.
10. Services to diagnose malfunctions or inoperability of the Software caused by changes, additions, enhancements, or modifications in the State's platform or in the Software.
11. Services to correct errors found to be caused by the State-supplied data, machines, or operator failure.
12. Operational supplies, including but not limited to, printer paper, printer ribbons, toner, photographic paper, magnetic tapes and any supplies in addition to that delivered with the System; battery replacement for uninterruptible power supply (UPS); office furniture including chairs or workstations.
13. Third-party software unless specifically listed on this Agreement.
14. Support of any interface(s) beyond Contractor-provided port or cable, or any services that are necessary because third party hardware, software or supplies fail to conform to the specifications concerning the Products.
15. Services related to the State's failure to back up its data or failure to use a UPS system to protect against power interruptions.
16. Any design consultation such as, but not limited to, configuration analysis, consultation with the State's third-party provider(s), and System analysis for modifications or Upgrades or Updates which are not directly related to a Residual Error report. F. The State hereby agrees to:
 1. Maintain any and all electrical and physical environments in accordance with the System manufacturer's specifications.
 2. Provide standard industry precautions (e.g. back-up files) ensuring database security, per the State's recommended backup procedures.
 3. Ensure System accessibility, which includes physical access to buildings as well as remote electronic access. Remote access can be stipulated and scheduled with the State; however, remote access is required and will not be substituted with on-site visits or proxies if access is not allowed or available.
 4. Appoint one or more qualified employees to perform System



Administration duties, including acting as a primary point of contact to the Contractor's Technical Support organization for reporting and verifying problems and performing System backup. At least one member of the System Administrators group must have completed the Contractor's End-User training and System Administrator training (if available). The combined skills of this System Administrators group includes proficiency with: the Products, the system platform upon which the Products operate, the operating system, database administration, network capabilities such as backing up, updating, adding, and deleting System and user information, and the client, server and stand alone personal computer hardware. The System Administrator will follow the Residual Error reporting process described herein and make all reasonable efforts to duplicate and verify problems and assign a Severity Level according to definitions provided herein. The State agrees to use reasonable efforts to ensure that all problems are reported and verified by the System Administrator before reporting them to the Contractor. The State will assist the Contractor to confirm that errors are not the product of the operation of an external system, data links between system, or network administration issues. If a Severity Level 1 or 2 Residual Error occurs, any State representatives may contact Contractor's Customer Support by telephone, but the System Administrator must follow up with Contractor's Customer Support as soon as practical thereafter.

5. In performing repairs under this Agreement, the Contractor may use parts that are not newly manufactured but which are warranted to be equivalent to new in performance. Parts replaced by Contractor will become Contractor's property.
 6. The State will permit and cooperate with the Contractor so that the Contractor may periodically conduct audits of the State's records and operations pertinent to the Services, Products, and usage of application and database management software. If the results of any such audit indicate that price has been understated, the Contractor may correct the price and immediately invoice the State for the difference (as well as any unpaid but owing license fees).
- G. If the State replaces, upgrades, or modifies equipment, or replaces, upgrades, or modifies hardware or software that interfaces with the covered Products, the Contractor will have the right to adjust the price for the Services to the appropriate current price for the new configuration.
- H. The State agrees not to attempt or apply any update(s), alteration(s), or change(s) to the database software without the prior approval of Contractor.

4.0 Hardware Upgrades

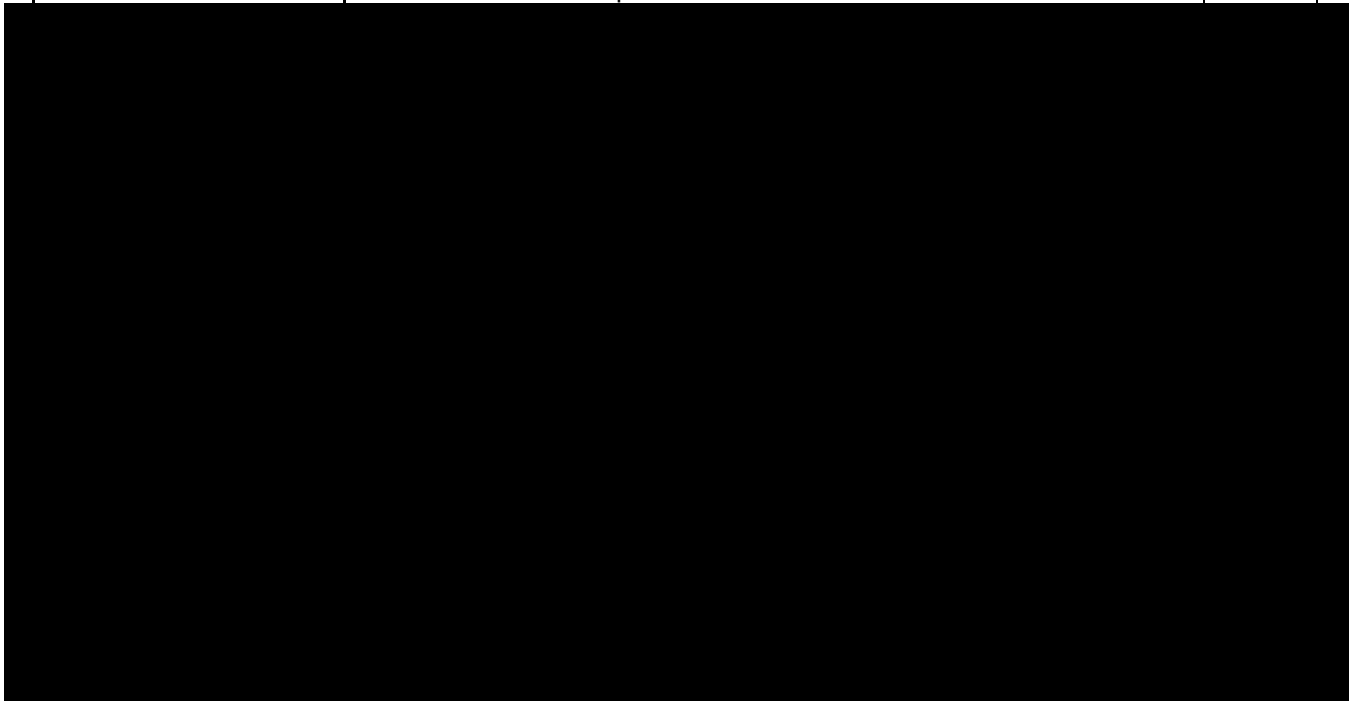


Hardware necessary for proper PremierOne functionality will be updated twice (2) during the contract at the intervals established by the State, all costs of which are included in this contract.

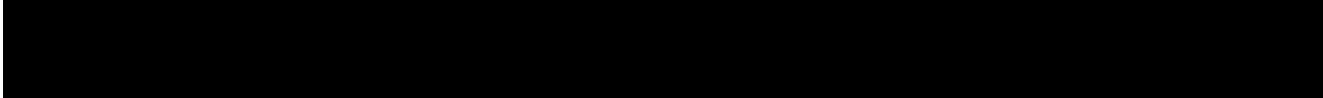
5.0 Example List

***Covered products and quantities to be updated annually by June 1.**

Product	Description	Qty
PREMIERONE CAD™	PremierOne Query Service Server License - with Basic Query State Interface	1
	PremierOne Reporting Service Server License	1
	PremierOne GIS Editing Client Plug-In License (for use with ESRI ArcGIS Editor)	1
	PremierOne CAD™ Server License (Primary)	1
	PremierOne CAD™ Dispatch (CAD Client & Mapping)	6
	PremierOne CAD™ Dispatch (CAD Client & Mapping) - SA 1172	5
MOTOROLA INTERFACES	E911 (Per Interface)	1
	Spectracom Netclock Interface	1
	Mobile Interface	1
	TDD Interface	1
	PTT & Emergency ID (Gold Elite Console)	1
PREMIERMDC™	PremierMDC™ Server (3001-3500 units)	1
	PremierMDC™ Clients (501+ units)	650
	PremierMDC™ In-house Client Software (additional copies)	24
	PMDC-PCMCIA Flashcard Media (32MB)	10
	State/NCIC/NLETS Interface (Included)	1
	CAD Interface Development- CAD to Motorola API9A	1



MA# 190000001544





MAINTENANCE AND SUPPORT AGREEMENT 806 (Incorporated 372(A)) TERM: 10/1/2019-9/30/202
CUSTOMER: Michigan V Public Safety Communications System (MPSCS)

1.1 GENERAL INFORMATION

This document describes the scope of work involved in providing upgraded PremierOne system software, and if specifically referenced, system hardware to support the Customer's upgrade to the latest generally available release of PremierOne application software, hereinafter referred to as Lifecycle services, throughout the duration of the maintenance and support period. The Lifecycle services are provided in accordance with the terms and conditions of the Motorola Solutions Inc. Maintenance and Support Agreement ("Agreement").

Per the terms of the Agreement, when and if a Standard Release version becomes available, Motorola will perform software upgrade services described in this Statement of Work up to four (4) during the Term and will perform hardware upgrade services and replacement hardware described in this Statement of Work to upgrade the system hardware twice (2) during the Term and in combination with the installation of a Standard Release, upon customer initiated request to the Customer Support organization. Upgrades will be scheduled in order of receipt, based on resource availability.

Nothing in this Statement of Work is meant to supersede, replace or amend the terms and conditions stated in the Motorola Solutions Inc. Maintenance and Support agreement.

1.2 UPGRADE SERVICES

Lifecycle Services are defined in scope as the labor services required to execute on the planning, delivering, testing and training of Motorola Standard Releases of software to the Customer when and if Standard Releases of software become available for those solutions components identified in Exhibit A Description of Covered Products contained within the Motorola Solutions, Inc. Maintenance and Support Agreement.

At the time of contracting, Motorola has identified the covered software products as follows:

- ◆ PremierOne Software inclusive of, where applicable,
 - PremierOne CAD™ and PremierMDC™

Except for the upgrade that includes new system hardware, unless specifically noted here, the existing hardware will be re-utilized with the upgraded PremierOne System software when feasible. Should changes in hardware or additional hardware be required for the new release, Motorola Solutions will notify Customer.

All upgrade activities will be coordinated and scheduled to occur at times that are mutually agreeable to the Customer and Motorola. Scheduling of upgrade events will be completed at a minimum of 30 business days prior to the commencement of upgrade activities.



1.3 UPGRADE CONSIDERATIONS

The scope of work described herein is based on the following considerations:

1. All parties recognize that the SOW is not necessarily formatted chronologically with contractual obligations defaulting to the project schedule.
2. Only those interfaces covered under the terms of the Maintenance and Support Agreement will be validated and or modified to ensure operational use with the upgraded PremierOne System software. Supported interface functionality is that which is described in the original interface specification document (ISD).
3. Prior to cutover, there may be periods of time during which interface functionality will not be available for production operations while testing is conducted with the new hardware.
4. If the upgraded software version supports enhanced interface functionality that is desired but not supported by the original interface, such enhanced functionality shall not be available unless specifically included in the scope described herein.
5. CAD user interface (UI) customization will be replicated from the current CAD UI.
6. Customer should be prepared to go to a “manual” mode during the periods of time when operations are moving from the existing system to the upgraded system.

1.4 KICKOFF TELECONFERENCE

In order to finalize the project schedules and procedures, the upgrade event will be initiated with a kickoff teleconference that includes key Customer and Motorola project participants.

The objectives of this task are:

- To introduce all project participants.
- Review roles of key participants.
- Review overall upgrade scope and objectives.
- Review the list of interfaces.
- Discuss client upgrade procedures and coordination.
- Review resource and scheduling requirements.
- Review and finalize project schedule with Customer.
- Review operational readiness and resumption of use criteria.

Motorola Responsibilities

1. Assign a Project Manager that will direct Motorola’s efforts and serve as the primary point of contact for the Customer.
2. Schedule and facilitate the kickoff teleconference.
3. Discuss GIS requirements, if applicable.
4. Maintain project communications with the Customer’s project manager.
5. Manage the efforts of Motorola project team and coordinate Motorola activities with the Customer’s project team members.
6. Coordinate and oversee the installation of required additional hardware and all licensed Motorola application software.



7. Deliver product release documentation.

Customer Responsibilities

1. Designate a project manager who will direct Customer's efforts and serve as the primary point of contact for the Motorola Project Manager.
2. Provide input to the final project schedule dates.
3. Identify the efforts required of Customer staff and assign appropriate resources to meet the Customer's task requirements described in this Statement of Work.
4. Liaison and coordinate with other partner agencies, other governmental agencies and the Customer's vendors, contractors and common carriers, as applicable.
5. Provide all network infrastructures. Motorola makes no provision for cabling or capital improvements to the installation environment and power consumption considerations that may be required to support the PremierOne solution.
6. Maintain responsibility for connectivity to all external systems.
7. In the event modifications to 3rd party systems to which PremierOne interfaces are required to maintain or enhance interface functionality, Customer is responsible for engaging and/or contracting with the 3rd party and any associated costs associated to effect such changes.
8. Act as liaison with all user agencies and other outside agencies, organizations and 3rd party vendors, if/as necessary.

Completion Criteria

This task is considered complete upon conclusion of the Upgrade Kickoff Teleconference.

1.5 HARDWARE AND SOFTWARE UPGRADE IMPLEMENTATION

The objective of this task is to conduct activities required for the upgrade of the PremierOne hardware and software. Motorola will procure and deliver the new system hardware and software to the primary site.

The new system equipment will be installed at the primary site where it will be tested and made available to the Customer for additional user testing and training. Upon acknowledgement that testing and training has been successfully completed, users will transition to the upgraded production system.

1.5.1 PremierOne Hardware and Software Upgrade

Motorola Responsibilities

1. Order hardware and software.
2. Stage system at Motorola facility.
3. Integrate and configure server and hardware components.
4. Backup and restore production database from existing system.
5. Ship system to Customer site.
6. Travel to perform installation tasks.
7. Configure interface connections, depending on connections Customer makes available.
8. Remotely review new features and functions.
9. Remotely conduct provisioning and functionality upgrade training.
10. Provide remote support for up to ten (10) business days while Customer tests system.

**Customer Responsibilities**

1. Provide and make available (during business hours, 8:00am to 5:00pm) remote connectivity and access to 3rd party systems for initial testing of environment.
2. Perform testing on system (up to 10 business days).
3. Train users on new or changed features and functions.
4. The Customer will ensure all firmware and BIOS on all customer provided hardware are at a currently supported level or the Customer may elect to contract with MSI for the services to perform such updates.

1.5.2 Cutover to Production System**Motorola Responsibilities**

1. Assist customer in developing cut-over plan to include plan for CAD and Mobile client updates.
2. Perform final backup and transfer of CAD database to new system.
3. Test system and subsystem interfaces with production connections to validate operation in accordance with the original ISDs.
4. Verify system readiness for Go-Live.
5. Support the transition of production operations to the upgraded system. Support will be provided on the day of the upgrade and during business hours for two days following the upgrade.

Customer Responsibilities

1. Provide and make available (during business hours, 8:00am to 5:00pm) the appropriate lines for production testing of interfaces.
2. Acknowledge system readiness for production cutover.
3. Execute the plan to install upgraded client software on CAD workstations and mobile devices.
4. Facilitate the transition of production operations to the upgraded primary system.

Completion Criteria

This task is considered complete when the production operations have transitioned to the upgraded primary system.

1.5.3 Upgrade Completion

Completion of the upgrade will be acknowledged by the Customer upon production operations of the upgraded software. The Customer will work with the support organization to update existing cases that are resolved with the upgrade.



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

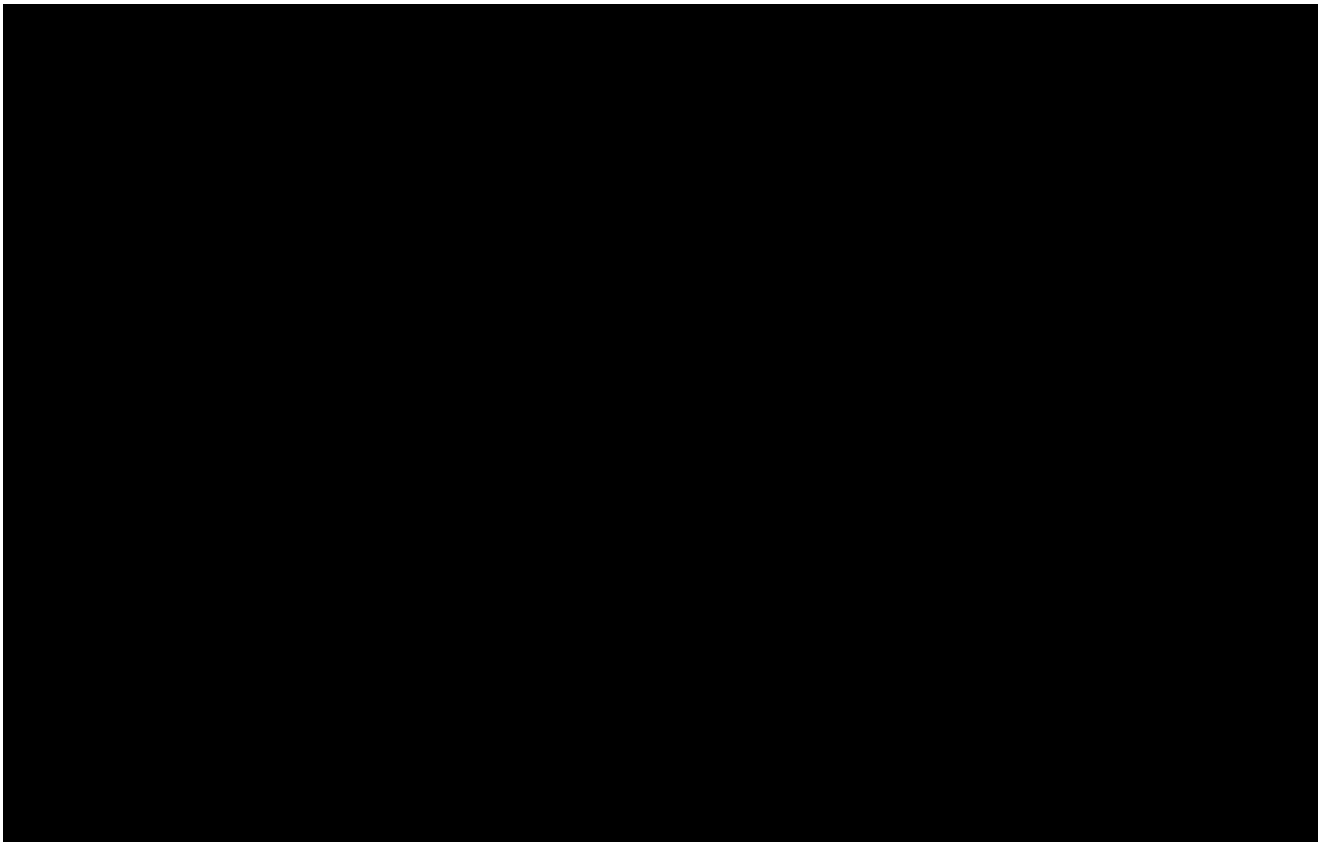
ATTACHMENT 4 to SCHEDULE A

On Premise Security Operations Center (OPSOC) Service Overview

Motorola Solutions, Inc.'s ("Contractor") On Premise Security Operations Center (OPSOC) is a highly customizable and feature rich security information and event management (SIEM) solution to allow local monitoring of security events of interest in an ASTRO 25 system. The OPSOC solution is built on the Correllog® SIEM correlation server however, it is a unique software installation package developed for Motorola Solutions, specifically designed and tuned for operation within an ASTRO 25 system.

Located within the network management subnet, the OPSOC server receives all system generated syslog messages from the centralized syslog server as well as simple network management protocol (SNMP) data from UEM. Messages are then correlated into security threats and alerts which can be configured to automatically generate administrator notifications, tickets for incident resolution and reporting.

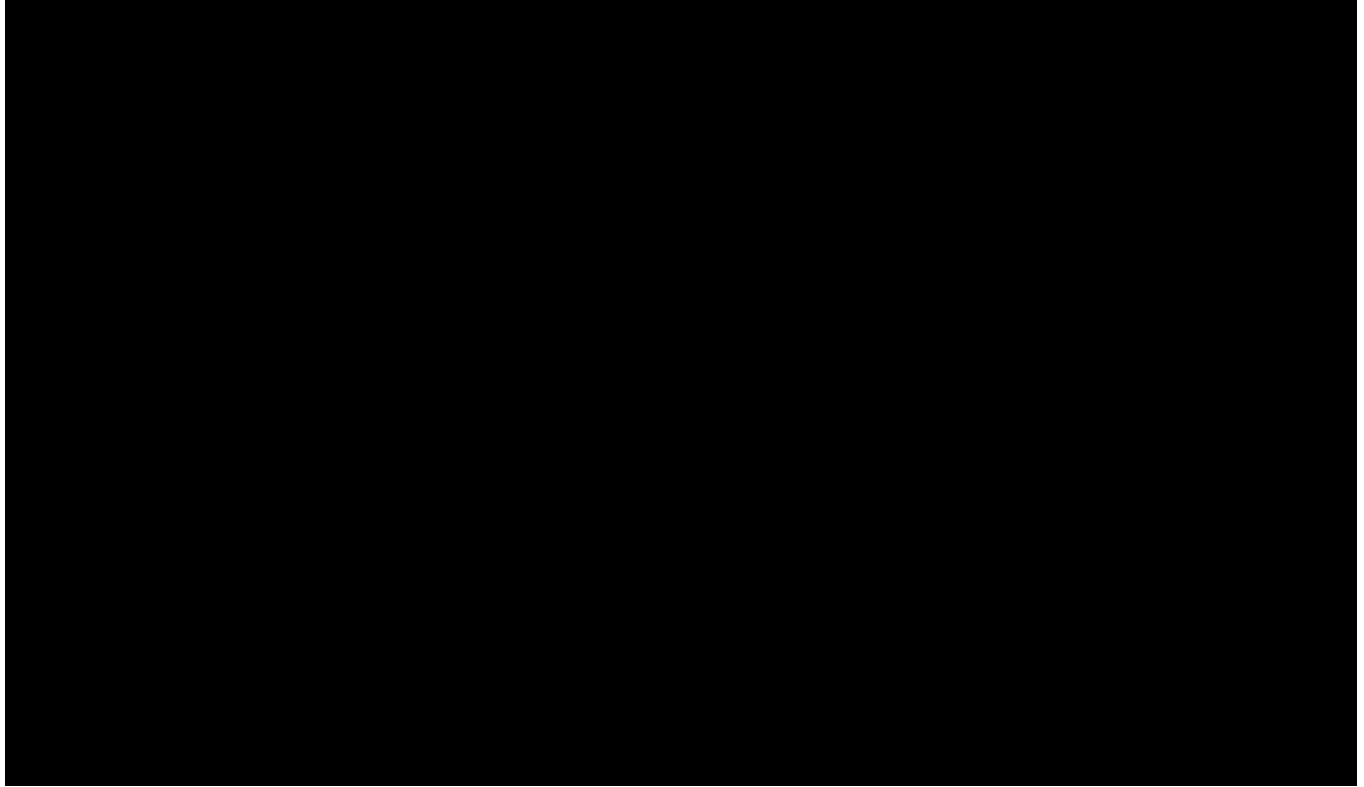
OPSOC can be deployed within single zone or multi-zone system configurations. The diagram below demonstrates a high-level architectural representation of OPSOC data collection from within a multi zone environment.





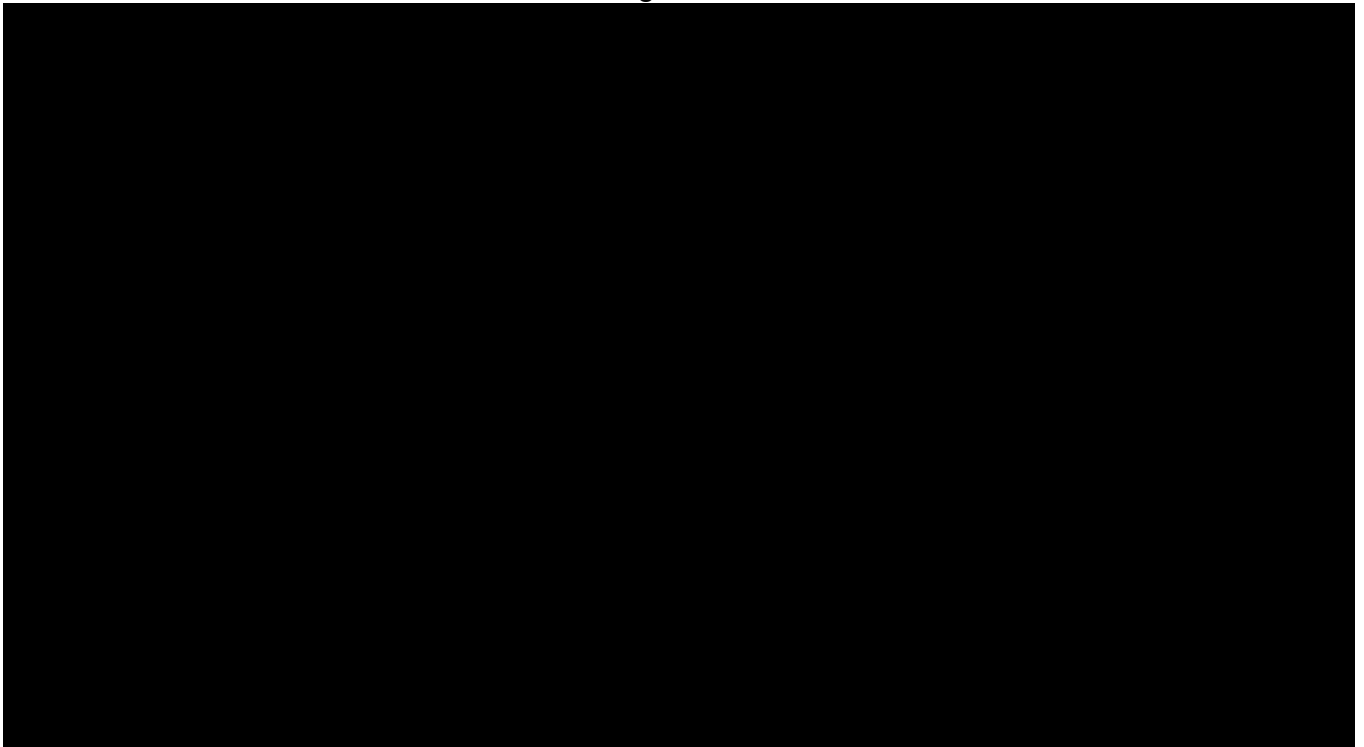
1.0. Description of OPSOC Services

The OPSOC service is made up of the following elements:



1.2. Server Integration

The OPSOC solution will be integrated into the ASTRO 25 network.





2.0. Scope

2.1. The Contractor's Responsibilities:

- A. Provide, maintain, and replace when necessary, hardware and software required for OPSOC to function correctly. HW and SW will always be fully supported by the OEM and will not be in an end of life situation.
- B. Full integration of the OPSOC solution into the ASTRO 25 system.
- C. Provide at the least, annual updates to the OPSOC application that may include application, dashboard and correlation rule updates. Updates may be more frequent should the need arise.
 - 1. *Note: State specific customization preservation cannot be guaranteed when performing updates to the core application. Motorola Solutions OPSOC technical support staff will provide guidance on how to mitigate this risk.*
- D. Provide an update mechanism that requires the minimum amount of downtime and end user input as possible.
- E. Provide access to OPSOC technical support staff. 10 hours is included annually for configuration and customization requests, additional hours may be purchased.
- F. OPSOC licensing is renewed annually. OPSOC technical support staff shall prove licensing media to the State.

2.2. The State's Responsibilities:

- A. Any changes to the default dashboards or standard configuration shall be carried out and maintained by the State. Detailed instruction manuals are available as well as access to OPSOC technical support staff to ensure that this can be carried out.
- B. Utilize the system as frequently as possible to check for any security events of interest or tickets that have been generated as a result of a correlation rule match.
- C. Investigate and close all security tickets generated in a timely manner, utilizing the access to security analysts included with this service if necessary.
- D. The State shall be responsible for application of licensing media on to the OPSOC server.
- E. Maintain log archives in accordance with local policy or compliance requirements.
- F. Maintain service in good standing.
- G. Return all equipment if service is terminated.



2.3 Disclaimer

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



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

**ATTACHMENT 5 TO SCHEDULE A
Technical Support**

1.1 TECHNICAL SUPPORT STATEMENT OF WORK

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

A. Scope

Technical Support service is available Monday - Friday 8:00am - 5:00pm Eastern time and 24 hours a day, 7 days a week for Critical and High Priority Incidents. See **Priority Level Response Goals Level Definitions** in **Section 1.6** below.

1. Calls requiring incidents or service requests will be logged in the Contractor's Customer Relationship Management (CRM) system.
2. The Contractor's Technical Support Operations will assign an impact level in accordance with the agreed Priority Level Response Goals Level Definitions stated in Section 1.7 of this document.
3. The Contractor will track the progress of each Incident from initial capture to resolution. Motorola will advise and inform the customer of the Incident progress and tasks that require further investigation and assistance from the customer's technical resources.
4. The State will provide a suitably trained technical resource that delivers maintenance and support to the MPSCS, and who is familiar with the operation of that system.
5. The Contactor will provide technical consultants to support the local resource in the timely closure of infrastructure, performance and operational issues.



B. Inclusions

Technical Support service will be delivered on all Contractor sold infrastructure including third-party products.

C. Limitations and Exclusions

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

1. Emergency on-site visits required to resolve technical issues that cannot be resolved with the SSC working remotely with the local customer technical resource.
2. Third party support for equipment not sold by Motorola.
 - a. System installations, upgrades, and expansions.
 - b. Customer training.
 - c. Hardware repair and/or exchange.
 - d. Network security services.
 - e. Network transport management.
 - f. Motorola services not included in this statement of work.
 - g. Any technical support required as a result of a virus or unwanted intrusion is excluded if the system is not protected against these security threats by Motorola's Pretested Security Update Service when applicable.

D. The Contractor has the following responsibilities:

1. Provide availability to the Motorola Solution Support Center [REDACTED] 24 hours a day, 7 days a week to respond to State's requests for Critical, High Priority Incidents. Refer to **Priority Level Response Time Goals, Section 1.6** for Medium, Low response times.
2. Respond initially to Incidents and Technical Service Requests in accordance with the response times set forth in the **Priority Level Response Time Goals, Section 1.6** of this document and the Incident priority levels defined in the **Priority Level Definitions, Section 1.7** of this document.
3. Provide caller a plan of action outlining additional requirements, activities or information required to achieve restoral/fulfillment.



4. Maintain communication with the customer in the field as needed until resolution of the Incident
5. Coordinate technical resolutions with agreed upon third party vendors, as needed.
6. Manage functionally escalated support issues to additional Motorola technical resources, as applicable.
7. Determine, in its sole discretion, when an Incident requires more than the Technical Support services described in this SOW and notify customer of an alternative course of action.

E. The State has the following responsibilities:

1. Provide the Contractor with pre-defined information prior to contract start date necessary to complete Customer Support Plan (CSP).
2. Submit changes in any information supplied in the Customer Support Plan (CSP) to the MPSCS NCC Manager.
3. Contact the SSC in order to engage the Technical Support service, providing the necessary information for proper entitlement services. Including but not limited to the name of contact, name of customer, system ID number, site(s) in question, and brief description of the problem including pertinent information for initial issue characterization.
4. Maintain suitable trained technical resources that provide field maintenance and technical maintenance services to the system, and who are familiar with the operation of that system.
5. Supply suitably skilled and trained on-site presence when requested by the SSC.
6. Validate issue resolution prior to close of the Incident in a timely manner.
7. Acknowledge that Incidents will be handled in accordance with the times and priorities as defined in the **Priority Level Definitions, Section 1.6** and in the **Priority Level Response Time Goals, Section 1.7** section in this document.
8. Cooperate with the Contractor and perform all acts that are reasonable or necessary to enable Motorola to provide the Technical Support.



9. Obtain at the State’s cost all third-party consents or licenses as required, but not being provided by the Contractor, to enable the Contractor to provide the Service.

F. Priority Level Definitions

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

Incident Priority	Definition
Critical	<p>Core: Core server failures Core Link failure</p> <p>Sites/Subsites: Entire Simulcast Not Wide Trunking ≥ 33% of Sites/subsites down ○</p>
High	<p>⌘ Consoles: Console positions down (≥ 33%) Console Site Link Down ⌘</p> <p>Sites/Subsites: < 33% of Sites/subsites down ≥ 33% of channels down ⌘</p> <p>Conventional Channels: ≥ 50% of conventional channels (CCGW) down ⌘</p> <p>Devices: Site Router/switch, GPS server down</p>
Medium	<p>Consoles: Console positions down (< 33% at a site)</p> <p>Sites/Subsites: < 33% of channels down</p> <p>Conventional Channels: □ Less than 50% of conventional channel down</p>
Low	<p>Consoles: Console positions down (< 33% at a site)</p> <p>Sites/Subsites: < 33% of channels down</p> <p>Conventional Channels: □ Less than 50% of conventional channel down</p>

G. Technical Support Priority Level Response Goals

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

Incident Priority	Response Time
Critical	A Motorola SSC Technician will make contact with the customer technical representative within one hour of the request for support being logged in the issue management system. Continual effort will be maintained to restore the system or provide a workaround resolution. Response provided 24 x 7.



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



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

**ATTACHMENT 6 to SCHEDULE A
Business Relationship Manager (BRM)**

1. General Requirements

The Business Relationship Manager (BRM) (Employee) will be a qualified employee of the Contactor who will meet the requirement and provide the services outlined in this attachment.

- A. The BRM will always remain the Contractor's employee even as they are assigned to MPSCS.
- B. The employee will at all time have authorization, under the applicable laws of the United States, to perform paid work in the United States.
- C. The assignment of a BRM to MPSCS does not constitute a partnership between the Contractor and the State or an agent of the other party for any purpose.
 - 1) Neither the State nor the Contractor will have the authority or power to bind the other, to act as agent of the other, or to contract on behalf of the other or to create a liability against the other in any way or for any purpose, except with the express written consent of the other.

2. Obligations

- A. The Contractor will:
 - 1) Assign this employee to carry out the activities and functions as required and hold the authorizations granted to them by MPSCS;
 - 2) continue to pay Employee 100% of their salary and other benefits, in accordance with the Contractor's policies;
 - 3) continue to reimburse Employee for all reasonable expenses incurred by Employee that are authorized under Motorola Solutions' travel and expense policies
 - 4) comply with all applicable laws, statutes and regulations regarding the Employee's employment; and
 - 5) Will maintain all necessary insurance coverage for any liability to or on behalf of Employee, as is generally the case for all other Contractor employees.
- B. The BRM is not entitled to enter into a written agreement on behalf of the Contractor without the express prior written consent of the Contractor.



- C. The BRM will work a normal work week (40 hours per week) and may take reasonable leave for statutory holidays and/or vacations.
- D. The State will provide the BRM with adequate, sufficient, and appropriate facilities and resources to enable them to perform the services. These facilities include but are not limited to:
 - 1) Workstation
 - 2) Lockable walled office
 - 3) Telephone
 - 4) Facilities and/or Security access badges where appropriate and as needed
 - 5) E-mail or access to an outside network
 - 6) MPSCS network/peripherals access for use for project purposes
- E. The State, during the term of this agreement and for a period of 24 months following the termination of this agreement, will not, without the prior written consent of the Contractor, directly or indirectly:
 - a. solicit, employ or retain, or cause another person or entity to solicit, employ or retain, an Employee who is employed by the Contractor or was employed by Contractor for the six (6) months preceding such solicitation, hiring or retention;
 - b. encourage the BRM to devote all his or her business time to the State; or
 - c. agree to hire or employ the Employee in question.

3. Confidentiality

The BRM may obtain and have access to confidential and proprietary information from both the State and the Contractor and:

- A. This information remains confidential and exclusive to the parties;
- B. All documents, plans, computer programs, specifications, files and any other written or machine-readable work produced by the BRM for MPSCS or for the Contractor shall belong to this part; and
- C. The Contractor and the State will comply with all applicable data protection laws.

4. BRM Job Description The

BRM will:

- A. Be the designated single point of contact for the State's MPSCS, into the Contractor, as well as the designated point of escalation throughout Motorola.
- B. Have authority and functional line reporting structure within the Contractor's organization to hold all the Contractor's resources accountable.



- 1) Report directly to the Motorola Regional Sales Vice President in which the State of Michigan falls within. Should the Motorola sales structure change, the State of Michigan shall be notified in writing of 30 days prior of such changes and the potential impact to the BRM role and the support for MPSCS.
 - 2) Reports directly to the MPSCS Director
 - 3) Convergence of the Contractor's business functions under one statewide program owner
 - 4) Collaborating and aligning with regional, statewide and local Contractor leadership and teams for one voice, one process and transparent communications between the Contractor and the State's MPSCS
 - 5) Facilitate communications between the Contractor and MPSCS and forecast major impacts to both organizations
- C. Foster, develop and maintain strong and positive relationships with the State's MPSCS & the Contractor by:
- 1) Providing ownership, accountability, leadership, vision and strategy between all parties
 - 2) Driving and owning process change to mutually benefit all parties
 - 3) Hold both the Contractor and the State accountable for deliverables, process, communications, resources, and commitments
 - 4) Escalating and provide visibility regarding the State's MPSCS challenges and roadblocks to the Contractor through the State's MPSCS management and director.
 - 5) Engage in all future Contractor and State add-on projects to help ensure resources and commitments are being met from both the Contractor and the State
- D. Continuously drive and coordinate technology roadmap and interface, assisting with Voice of the Customer (VOC) and keep the State informed of major technology changes
- 1) Work internally with the Contractor's stakeholders (sales, service, system integration, software and product groups), and externally with MPSCS and other related customers to:
 - a. Coordinate technology roadmap alignment.
 - b. Communicate the State's MPSCS technology requirements and deliverables
- E. Align the State with the correct Motorola resources/SMEs as requested by the MPSCS
- F. Be informed of new solutions for feasibility, interoperability and sustainability



- G. Coordinate the verification and validation testing of applications and HW to adhere to the State's defined standards.
- H. Coordinate with Motorola sales to ensure solutions sold can be integrated or supported by the MPSCS. Further ensure resources assigned are delivering what is required and expected by the partnership between the Contractor and State
- I. Will be a full-time resident in Michigan
- J. Be onsite (Lansing MPSCS headquarters) minimum of 3 days a week.
 - 1) Unless on PTO
 - 2) Unless attending or engaged in training
 - 3) Unless weather is hazardous for driving
 - 4) Unless traveling for business or MPSCS meetings

5. Governance Model

To contribute to the success of the BRM initiative we propose the development of the following governance approach to manage the MPSCS/MSI program.

For your consideration.

360° degrees of Delivery - A Governance Approach

Effective relationships are built on a 360° strategy encompassing both proactive and reactive elements. **Reactive** elements enable effective management of tactical concerns while **Proactive** elements enable strategic management.

The traditional Reactive elements are the mechanisms which support the day to day delivery and respond when service issues are reported. These mechanisms drive resolution and communication also serving as the foundation for continuous service improvements and enhanced value. Call Centers, Service Desks and remote automated monitoring are typical mechanisms to ensure service issues are addressed and service maintained.

Proactive elements are equally essential and form the basis of the strategic relationship and Partnership. A core component is an effective, well designed and managed Governance approach. The term "**Governance**" takes on many forms and when well constructed enables progressive levels of interaction, accountability, and action. A key success factor at each level of governance is ensuring the participants are enabled to make decisions and take actions aimed at delivering the service and enhancing the partnership.

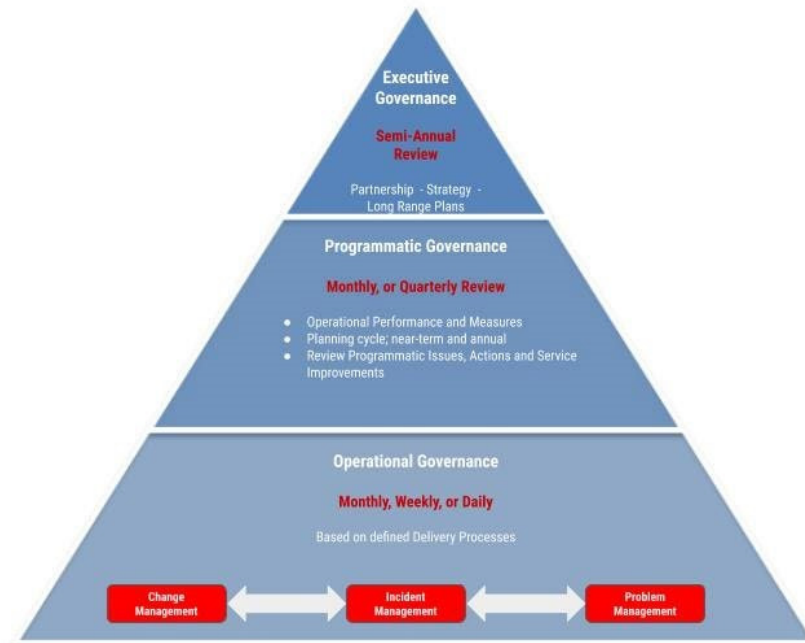
The Governance Pyramid

An effective view of good governance is the "**Governance Pyramid.**" The Pyramid represents the increasing levels of management and an elevating view of oversight. The pyramid is built on three tiers comprising:



- Operational Governance,
- Programmatic Governance, and
- Executive Governance

This tiered approach enables delivery operations and issues to be focused at the level best enabled to resolve, with effective escalation when necessary.



Operational Governance

The foundation of the governance pyramid is **Operational Governance** comprised of the established mechanisms and processes delivering the services. Within each process are local execution, governance, review and measurement mechanisms that enable operational management to maintain service. A key success factor is the ability to demonstrate to stakeholders and MPSCS that the committed services are delivered to agreement and expectations. The cadence of Operational Governance activities varies from process to process yet are well defined, documented, and enabled. The make up of this governance tier is typically the execution delivery and quality related managers accountable for the day to day operations. The vehicles for participation are typically Forums or Governance Boards.

Programmatic Governance

Serving as a higher level oversight **Programmatic Governance** focuses on reviewing the delivery of services and improving the service when gaps occur in delivery. The general focus is on delivery themes such as performance reviews, service improvement activities, and service enhancements which brings a more holistic view across operations. This governance tier may also engage and manage specific single delivery issues based on escalation or special sensitivity of the issue. Being a more oversight function the cadence is typically monthly or quarterly based



on the history of delivery and other management factors. The make up of this governance tier is typically the senior managers over the delivery execution areas, senior managers over shared, often referred to as “horizontal” or “cross functional” support organizations, and internal relationship managers. Participation is carefully designed to include the resources who are empowered to make critical decisions and take specific actions. The vehicle for participation is typically a Forum or Governance Board meeting.

Executive Governance

Essential to the relationship and governance over the pyramid is strong **Executive Governance**. Focused particularly on the partnership and the strategic plans this tier is designed to safeguard and maintain a healthy interaction among the top decision makers. When necessary through escalation from the Programmatic Governance tier Executive Governance may also engage in supporting resolution of specific critical delivery issues or other concerns. As the ultimate decision makers for both Partners the make up of this tier is typically critical and essential executive level resources. The cadence of Executive Governance activities is typically semi-annual so as to best align with both Partners internal planning and strategic cycles. The vehicle for participation is typically a Forum or Governance Board meeting. Additionally, mechanisms are established to allow for “off cycle” interactions to address concerns and issues in a time effective manner.

Making Governance Operational

The most common and effective approach to making a governance framework operational is to establish and agree upon a **Governance Charter** at the beginning of the partnership. The Charter primarily addresses the Executive Governance while referencing the governance tiers within the overall framework. The Charter defines the agenda, cadence and specific participation for the Executive Governance meetings, any communication and tracking mechanisms applicable, and general Guiding Principles for the Executive Governance Forum. Best practice is to include mechanisms for off cycle engagement in the event of major situations or issues which best not be deferred to the normal cadence.

Summary

When effectively empowered, executed and managed the Governance approach enhances both the delivery of services and the partnership. As a critical part of good delivery the result is 360° degrees of delivery and Partnership.



**Michigan's Public Safety Communications System (MPSCS) Continued
System
Updates, Equipment Maintenance and Upgrades, and Ancillary Systems
Products**

**ATTACHMENT 7 TO SCHEDULE A
Security Addendum**

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum.



The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and



conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information
Services Division, FBI 1000
Custer Hollow Road
Clarksburg, West Virginia 26306



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

ATTACHMENT 8 TO SCHEDULE A Motorola Customer Support Plan for Technical Support, SUS and SUAll

The following table lists the revision history of this document. The information contained in this document is subject to revision and is intended to be reviewed and updated periodically.

TABLE OF CONTENTS

1. Introduction
2. Overview of Services
3. Warranty and/or Service Information
4. How to Obtain Services
5. Above Contract Services
6. Glossary of Terms
7. Severity Level Definitions
8. Customer Contacts
9. Service Call Procedure
10. Site Summary

1. Introduction

Motorola has a corporate-wide standard in place which we refer to as 5NINES: SYSTEM AVAILABILITY. Our ability to provide highly available, easy-to-use systems is critical to our fundamental objective of total customer satisfaction and our position as a communications industry leader. 5NINES, or 99.999% availability (no more than 5 minutes total downtime per year), is the telephony standard to which all Motorola wireless systems aspire. We are committed to a new design culture, ease of use and operational simplicity, robustness metrics, and common platforms and network architecture.

The Terms and Conditions of your Agreement and all its other Exhibits will take precedence over this Customer Support Plan. In case of any contradiction, please contact the Motorola representative(s) below.

Customer Support Manager

Your Motorola Customer Support Manager provides coordination of support resources to enhance the quality of service delivery and to ensure your satisfaction. The Customer Support Manager (CSM) is responsible to oversee the execution of your support contract (maintenance or warranty) by serving in the role of customer advocate. They serve as a point of contact for issue resolution and escalation, monitoring of our contractual performance, providing review and analysis of process metrics and fostering a relationship for continuous improvement with



customers. Any changes to the information in this document should be communicated to your Customer Support Manager as soon as possible.

Your Customer Support Manager is: Dave
Woitylko

Account Manager

Your Account Manager serves as your contact for information on new products and services, expansion of communications to meet growth needs for your organization and ensure your satisfaction.

Your Account Manager is: Rich

2. Overview of Services

This section briefly describes the services MPSCS will receive under your contract.

Technical Support

Technical Support is available 7 days a week, 24 hours a day for Severity 1 issues, as defined in Section 7. The Motorola System Support Center's (SSC) staff will work with your local service organization or technicians to handle questions related to your Motorola 2-way communications system. The SSC's System Technologists may dial into a system to more clearly define a problem and determine the area of failure in order to decide on the most suitable action plan. If the problem is beyond the scope of the SSC's staff, they will contact key personnel who are involved with the design, development, and manufacture of your communication products for resolution.

Security Update Service

Security Update Service provides updates of the latest anti-virus definition, intrusion signature files and OS Patches that have been pre-tested on a Motorola test system to ensure they do not interfere with radio system functionality. Pre-tested updates will be made available as necessary, however, an outbreak of malicious code that is deemed a significant threat to the Astro 25 radio network will cause a priority test cycle to occur which will release anti-virus definition updates

System Upgrade Agreement II (SUA II)

Motorolas System Upgrade Agreement (SUA II) is a comprehensive approach to technology refreshment of the ASTRO 25 system, incorporating hardware, software and implementation services required to update the ASTRO 25 system. SUA II provides available system release software for Motorola and third-party infrastructure products; radio subscriber units (if purchased), product programming software, as well as commercial OS patch updates. As system releases become available, Motorola agrees to provide the Customer with the software, hardware and implementation services required to execute up to one system infrastructure upgrade in a twoyear period for their ASTRO 25 system.



3. Warranty and/or Service Agreement Information

Customer Number: [REDACTED]

Billing Tag: [REDACTED]

Service Agreement Information

Infrastructure Warranty Service Agreement number: [REDACTED]

Fixed equipment Warranty start date: 10/1/2018 Fixed

equipment Warranty end date: 9/30/2019

4. How To Obtain Services

How to Obtain Technical Support

Action	Information
Call the System Support Center.	[REDACTED]

Case created	Caller will receive a Case number
Technical Support Response Times	<p><u>RESPONSE*</u></p> <p>Severity 1: Within 1 hour Severity 2: Within 2 hours Severity 3: Within 24 hours</p> <p>* Severities Defined in Section 7</p>

Problem Diagnosis & Issue Resolution	<p>The SSC's System Technologists may dial into a system to more clearly define a problem and determine the area of failure in order to decide on the most suitable action plan.</p> <p>If the problem is beyond the scope of the SSC's staff, they will contact key personnel who are involved with the design, development, and manufacture of your communication products.</p>
Case Closed	Upon resolution of the issue, the SSC will close the Case.



How to Obtain Security Update Service

Action	Information
Updates	Motorola will pre-test the latest security software updates and make them available on the Motorola website upon successful completion of testing.
High Priority Updates	Motorola will pre-test urgent anti-virus updates and make them available on the Motorola website within 24 hours of commercial supplier's updates being available.
Notification	<p>Email notification confirming availability of updates will be sent to: Security Contact: MPSCS NCC</p> <div data-bbox="576 1012 1052 1144" style="background-color: black; width: 100%; height: 100%;"></div>
Download Updates	<p>Log into Motorola Website at</p> <div data-bbox="584 1255 1409 1297" style="background-color: black; width: 100%; height: 100%;"></div> <ol style="list-style-type: none"> 1.) Enter User ID 2.) Enter Your Password <p>Download pre-tested updates from the website (instructions for downloading or obtaining updates are available on the website)</p>



How to Obtain Software Upgrade Agreement Releases (SUA II)

Action	Information
Receive Bulletins from Motorola	Bulletins will be made available on the Motorola Website on a bi-annual basis.
Contact your Motorola Customer Support Manager or Customer Account Manager	They will then call the System Support Center at [REDACTED] to request the upgrade, and open an Upgrade Case

Above Contract Services

Services that need to be performed that are not covered by the Agreement are considered 'above contract' and are billable to MPSCS. Any above contract work must be authorized or work will not be billable and cannot be performed. Please refer to your Agreement for the Statements of Work and Terms and Conditions for the services that MPSCS has purchased

The following person will be contacted for approval on above contract work:

Above Contract Customer P.O. Authorization: Name:

Pete Langenfeld

Phone: 517-284-4105

Email: langenfeldp@michigan.gov

6. Glossary of Terms and Acronyms

CASE NUMBER: The number assigned to a customer's request for service. The SSC Call Center electronically tracks all Case Numbers to assure customer satisfaction.

CSM: Customer Support Manager

CSP: Customer Support Plan

ETA: Estimated time of arrival is an estimate of when the field technician will arrive at the customer's site.

FRU (Field Replaceable Unit): A FRU is a Field Replaceable Unit which is any module or board which can be removed from a piece of fixed equipment and exchanged with an identical module or board.

IDO: Infrastructure Depot Operations

MOTOROLA LOCAL SERVICE PROVIDER: A Motorola authorized service provider or a Motorola Field Technical Representative.

RA: Return Authorization needed by the System Support Center prior to sending equipment in for repair.

RESPONSE: Response times are defined as having an on-site technician, a remote systems technologist or a remote network specialist having taken assignment of the issue and working on the system.



RSC: Radio Support Center

RSS: Radio Service Software

SEVERITY: Each incoming call is assigned a severity level of Severity One, Two, or Three. Severity levels determine the Response Time Commitments. See Section 7 for your Severity Level definitions.

SSC: System Support Center

7. Priority Level Definitions

Priority Level Matrix	
Priority Level	Problem Type (If applicable)
1. Critical	Major System Failure Dispatched 7 x 24 x 365 days. 33% degraded
2. High	Significant System Impairment Dispatched 8 x 5 Monday - Friday, standard business days
3. Medium	Technical Question = Upgrades or intermittent problems, System problems presently being monitored Parts Question Technician is not on site, has questions concerning a problem. Work to be performed at a later time. 8 x 5 Monday - Friday, standard business hours
4. Low	Scheduled Maintenance, Scheduled upgrades

8. CUSTOMER CONTACTS

Please contact CSM if any of the information provided below has changed.

Above Contract PO Authorization:
 Pete Langenfeld 517-284-4105
 langenfelp@michigan.gov

Contacts for Service Escalations:
 Josh Drazkowski 517-284-4068
 drazkowskij@michigan.gov

Mark Sandberg 517-284-4086
 sandbergm@michigan.gov

Customer Communications Director
 Brad Stoddard 517-284-4101
 stoddardb@michigan.gov



9. Service Call Procedure for Fixed Infrastructure

Step	What you need to do:	Information to Provide
1	Call the System Support Center.	
2	Provide Your Customer Name	
3	Type of Request	
4	Provide System & Site ID #	
5	Identify the Severity Level	
6	Your Name and Telephone Number	
7	Description of the Problem/Failure	
8	Record the Service Case Number provided to you by Motorola Call Center Operations for service call tracking purposes.	
	If on site support is required to resolve the service request, the Motorola Call Center Operations will dispatch the appropriate local field service provider.	
	To inquire on the Status of a Service Call...	
1	Call Motorola Call Center Operations	
2	Provide Your Customer Name	
3	Provide Type of Request	
4	The Service Case number assigned at the time the service call was opened.	

SEVERITY LEVELS

Standard Severity & Response Times

Level	Response	Definition
1 - Critical	4 hour Response	System/site down or extremely degraded
2 - High	4 hour Response*	Degraded system/site
3 - Medium	1 day Response*	Non emergency, non user effecting
4 - Low	1 day Response*	Scheduled Maintenance, Scheduled upgrades

*Standard Business Days, Mon-Fri 8:30 a.m. - 4:30 p.m.. Local Time, excluding Motorola holidays.

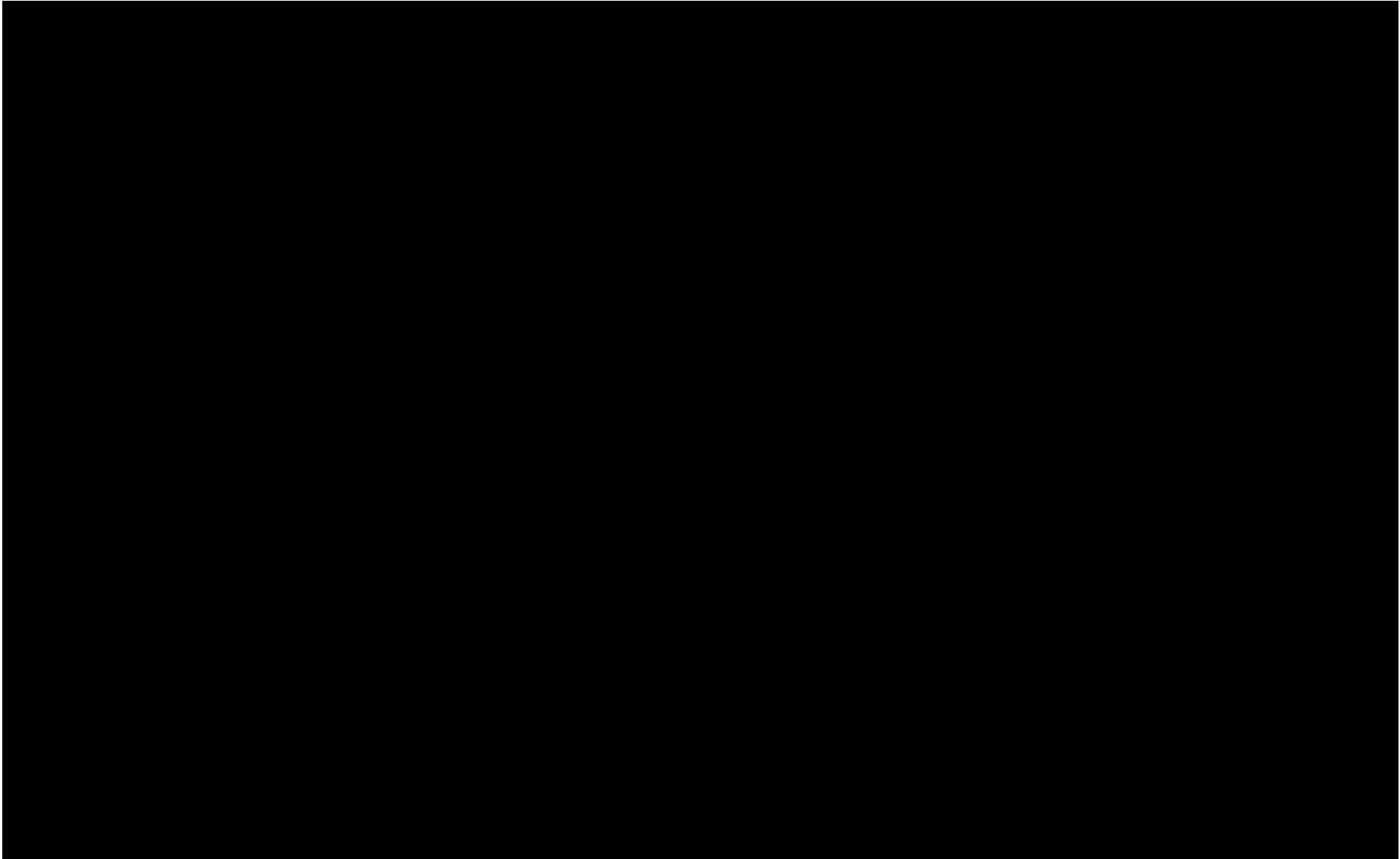


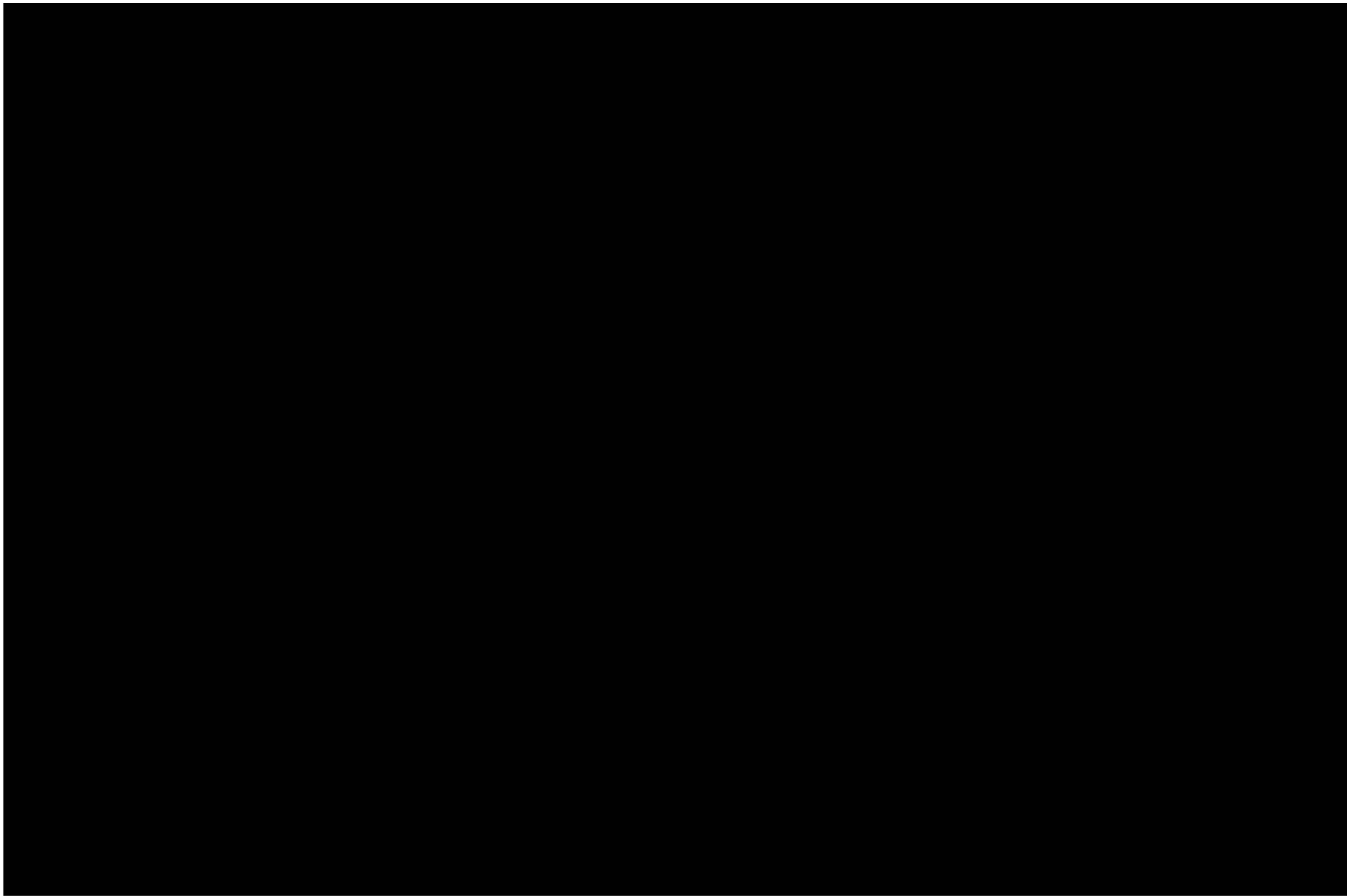
10. **Site Summary - (Technical Support Entitlement)**

Tables start on following page.



10. Site Summary Report (Technical Support Entitlement)





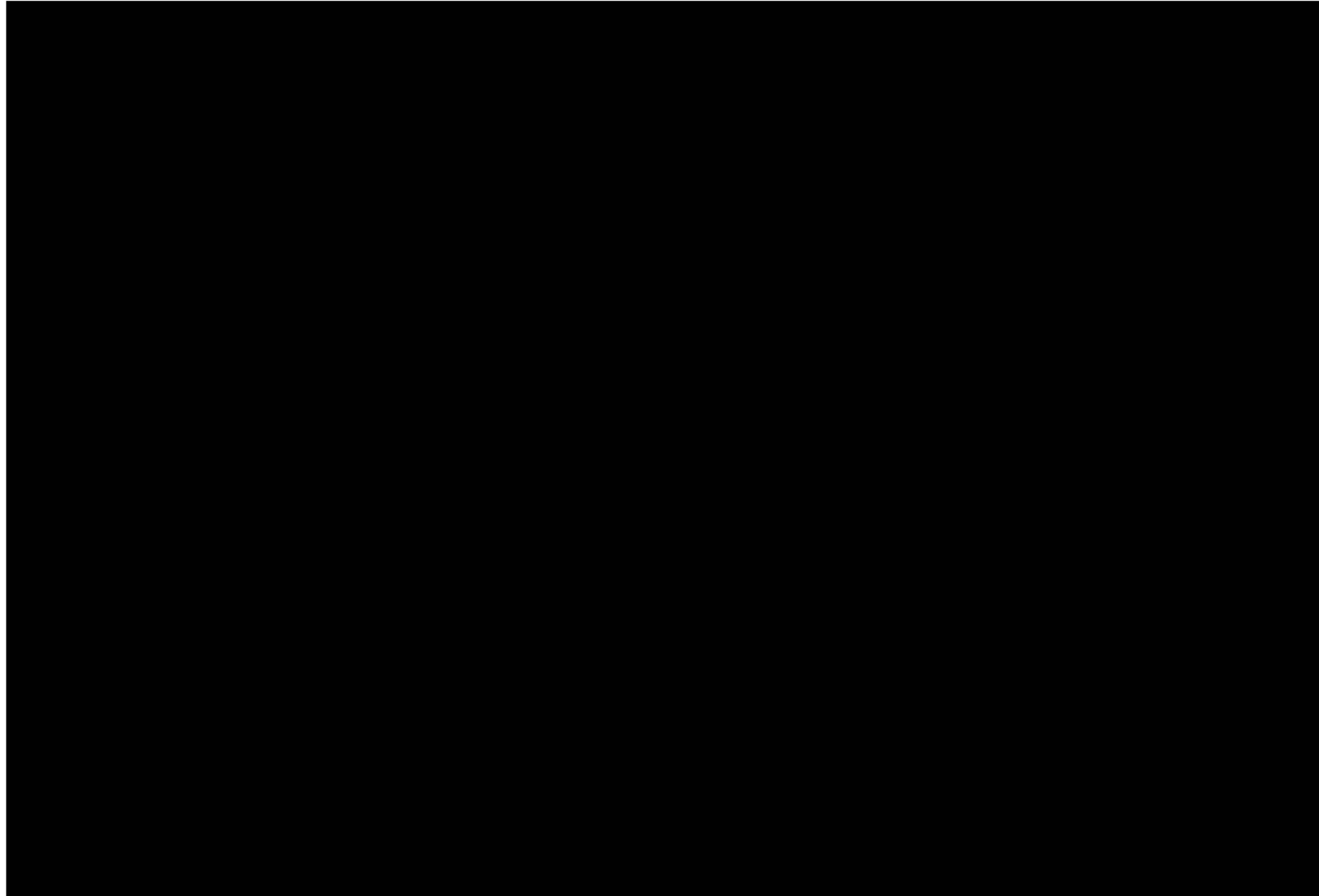














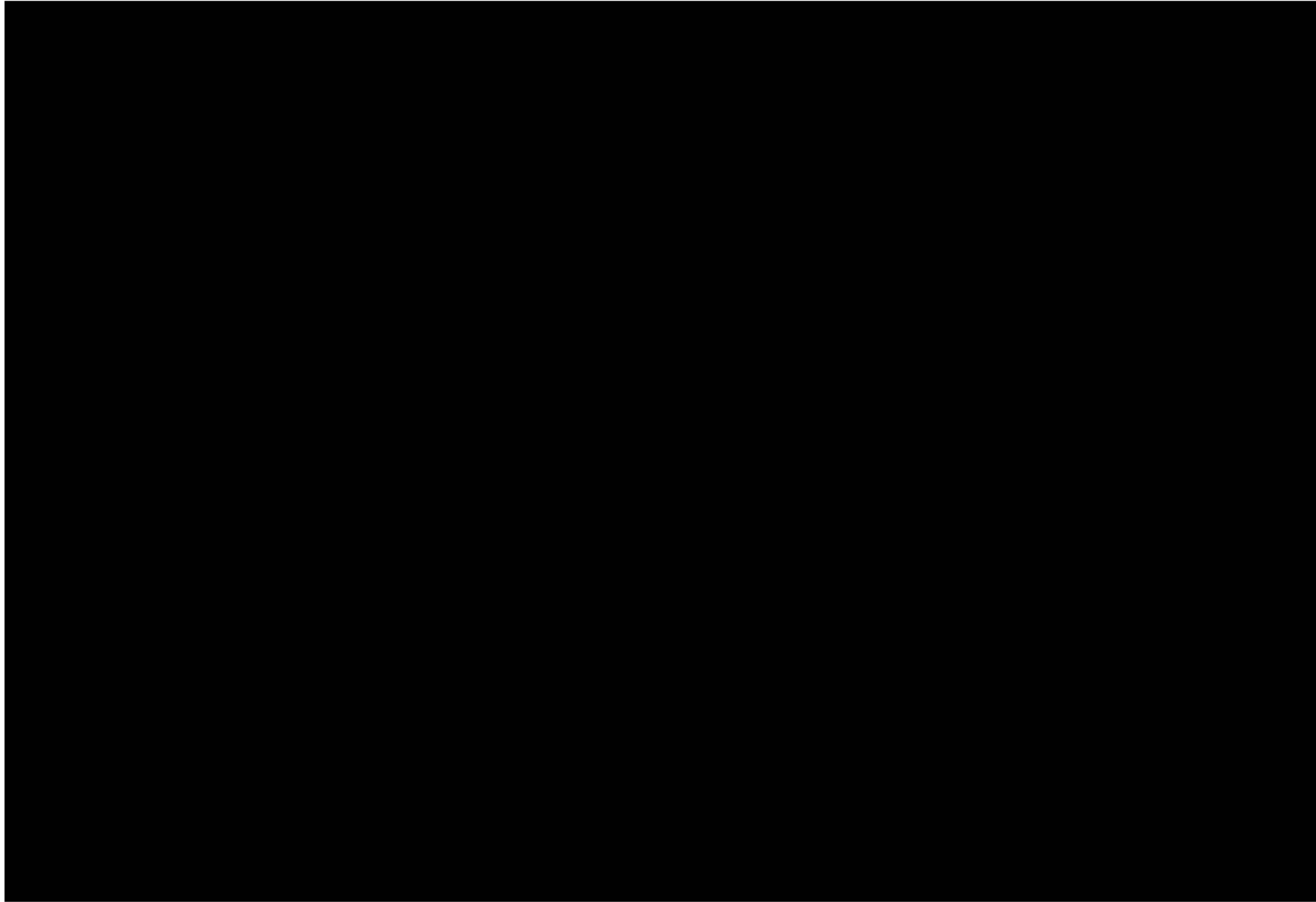


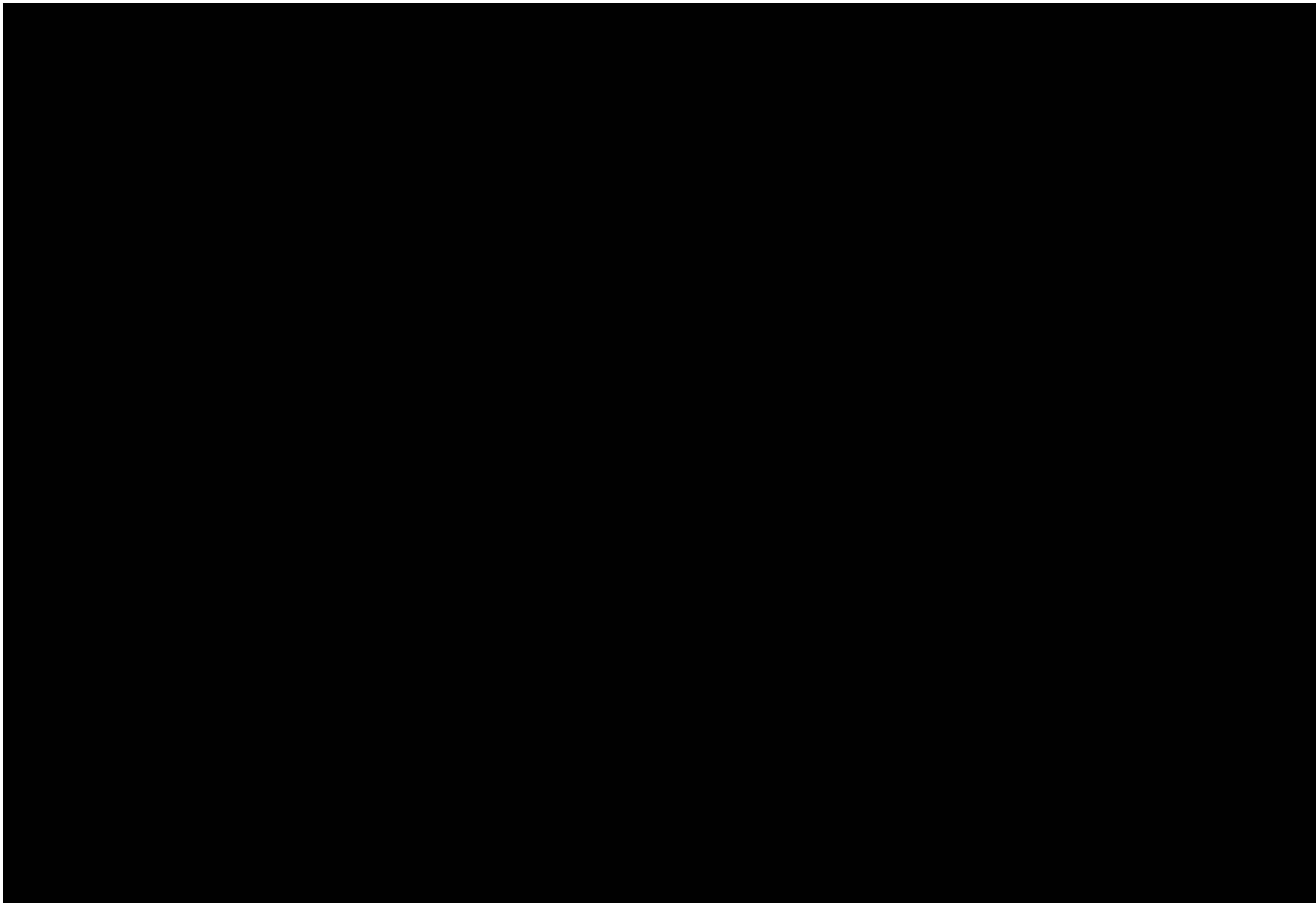
















Michigan’s Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

SCHEDULE B – PRICING

MAINTENANCE AND SUPPORT PRICING

Component		October 1, 2019	October 1, 2020	October 1, 2021	October 1, 2022	October 1, 2023	October 1, 2024	October 1, 2025	October 1, 2026	October 1, 2027	October 1, 2028	TOTAL
MPSCS ASTRO LIFECYCLE	System Upgrade Agreement II (SUA II)	\$ 4,666,781.89	\$ 5,119,186.80	\$ 5,570,726.31	\$ 5,900,187.68	\$ 6,460,906.70	\$ 6,502,411.06	\$ 6,545,043.90	\$ 6,589,066.01	\$ 6,634,415.11	\$ 6,681,002.78	\$ 60,669,728.24
	Security Update Services (SUS)	\$ 100,785.87	\$ 103,809.45	\$ 106,923.73	\$ 118,189.84	\$ 121,735.54	\$ 125,387.60	\$ 135,019.65	\$ 139,070.24	\$ 143,242.35	\$ 147,539.62	\$ 1,241,703.89
	Technical Support (TS)	\$ 252,878.41	\$ 260,464.76	\$ 268,278.70	\$ 296,546.12	\$ 305,442.50	\$ 314,605.77	\$ 338,773.22	\$ 348,936.41	\$ 359,404.51	\$ 370,186.64	\$ 3,115,517.03
	OPSOC	\$ 34,839.75	\$ 35,884.94	\$ 36,961.49	\$ 40,855.97	\$ 42,081.65	\$ 43,344.10	\$ 46,673.71	\$ 48,073.92	\$ 49,516.14	\$ 51,001.63	\$ 429,233.31
	Business Relationship Manager (BRM)	\$ 260,000.00	\$ 267,800.00	\$ 275,834.00	\$ 284,109.02	\$ 292,632.29	\$ 301,411.26	\$ 310,453.60	\$ 319,767.21	\$ 329,360.22	\$ 339,241.03	\$ 2,980,608.62
	TOTAL	\$ 5,315,285.91	\$ 5,787,145.95	\$ 6,258,724.24	\$ 6,639,888.63	\$ 7,222,798.67	\$ 7,287,159.80	\$ 7,375,964.08	\$ 7,444,913.79	\$ 7,515,938.33	\$ 7,588,971.70	\$ 68,436,791.09
MPSCS PREMIER**	PremierOne CAD		\$106,678.14	\$109,878.36	\$119,812.29	\$123,406.92	\$127,108.85	\$135,644.68	\$139,714.22	\$143,905.79	\$148,222.50	\$ 1,154,371.75
	PremierMDC	\$ 162,778.86	\$ 150,358.48	\$ 154,869.30	\$ 171,187.28	\$ 176,322.96	\$ 181,612.64	\$ 195,563.48	\$ 201,430.32	\$ 207,472.88	\$ 213,696.68	\$ 1,815,292.88
	Upgrade - Hardware/Software/Services		\$ 142,848.92	\$ 142,848.92	\$ 153,301.28	\$ 153,301.28	\$ 153,301.28	\$ 160,269.52	\$ 160,269.52	\$ 160,269.52	\$ 160,269.52	\$ 1,386,679.76
	TOTAL	\$ 162,778.86	\$ 399,885.54	\$ 407,596.58	\$ 444,300.85	\$ 453,031.16	\$ 462,022.77	\$ 491,477.68	\$ 501,414.06	\$ 511,648.19	\$ 522,188.70	\$ 4,356,344.39
GRAND TOTAL		\$ 5,478,064.77	\$ 6,187,031.49	\$ 6,666,320.82	\$ 7,084,189.48	\$ 7,675,829.83	\$ 7,749,182.57	\$ 7,867,441.76	\$ 7,946,327.85	\$ 8,027,586.52	\$ 8,111,160.40	\$ 72,793,135.48
MPSCS Existing Credits	Credit #1 - System Manager	\$ (154,291.00)										\$ (154,291.00)
	Credit #2 - WAVE Activation Fee	\$ (1,814.40)										\$ (1,814.40)
	Credit #3 - WAVE Hosting	\$ (6,900.00)										\$ (6,900.00)
	Credit #4 - Subscriber Activation	\$ (53,750.00)										\$ (53,750.00)
	GRAND TOTALS OF CREDITS	\$ (216,755.40)										

** CAD Workstations NOT included in pricing



DISCOUNT OFF LIST PRICING

Category	Discount % off List ^{#*}
Mobiles and Portables	
Any Qty Any Configuration	25%
Qty 1-49 (Minimally Configured with TDMA, DES-OFB/AES, and Multi-Key)	30%
Qty 50-99 (Minimally Configured with TDMA, DES-OFB/AES, and Multi-Key)	35%
Qty 100+ (Minimally Configured with TDMA, DES-OFB/AES, and Multi-Key)	40%
Fixed Stations	25%
Dropship **	10%
Consoles	25%
ASTRO and SmartZone Equivalent	25%
Fixed Network Equipment ***	25%
Spare Parts ***	25%
Accessories and Aftermarket ***	25%
PSA/CAD	20%
All other Motorola manufactured products not listed or becoming available for sale after 10/1/19	15%

- Extended Warranty, where applicable, is not included

* - Applicable to products available for sale as of 10/1/19

** Defined as any non-Motorola product.

*** Defined as Motorola products.

**CATEGORY DESCRIPTIONS:**

1. Mobile and Portable. Includes but are not limited to:
 - a. Mobile Radios- which is a fixed mount unit installed into a vehicle.
 - b. Portable Radios- which are personal radios
 - c. Console Radio- which are at dispatch centers or established for back up using 120v.

2. Fixed Stations. These are the large rack mounted radios located at radio tower sites, and receivers.

3. Dropship. Includes all items that the Contractor sells or distributes but has been manufactured by other companies. These items include, but are not limited to;
 - a. Microwave Equipment
 - b. Antenna Systems
 - c. Site Shelters
 - d. Third party hardware or software

4. Consoles. Includes the 911 dispatch consoles.

5. ASTRO and SmartZone. Includes the system infrastructure hardware, software and software licenses, located at the system master sites, which run the P25 Radio System.

6. Fixed Network Equipment. Includes all system infrastructure IP networking hardware, including but not limited to:
 - a. Routers
 - b. Switches
 - c. Firewalls

7. Spare Parts. To repair any items sold.



8. Accessories and Aftermarket. Includes but is not limited to such items as:
 - a. Belt clips
 - b. Remote speaker mics
 - c. Batteries

9. PSA/CAD. PSA stands for Public Safety Applications and CAD stands for Computer Aided Dispatch. This category includes but is not limited to such items as:
 - a. CAD systems software
 - b. Records management software



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

**SCHEDULE C
SOFTWARE TERMS FOR ON-SITE HOSTING**

1. Definitions. In addition to the definitions found in the Contract Terms, for the purposes of this Contract, the following terms have the following meanings:

"Authorized Users" means all Persons authorized by the State to access and use the Software under this Contract, subject to the maximum number of users specified in the applicable Statement of Work.

"Harmful Code" means any: (a) virus, trojan horse, worm, backdoor or other software or hardware devices the effect of which is to permit unauthorized access to, or to disable, erase, or otherwise harm, any computer, systems or software; or (b) time bomb, drop dead device, or other software or hardware device designed to disable a computer program automatically with the passage of time or under the positive control of any Person, or otherwise prevent, restrict or impede the State's or any Authorized User's use of such software.

"Integration Testing" has the meaning set forth in **Section 4.2(c)**.

"Open-Source Components" means any software component that is subject to any open-source copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

"Open-Source License" has the meaning set forth in **Section 2.3**.

"Operating Environment" means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in the Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software and system architecture and configuration.

"Specifications" means the specifications for the Software set forth in the applicable Statement of Work and, to the extent consistent with and not limiting of the foregoing, the Documentation.

"State Materials" means all materials and information, including documents, data, know-how, ideas, methodologies, specifications, software, content and technology,



in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

“Support Services” means the software maintenance and support services Contractor is required to or otherwise does provide to the State pursuant to Contractor’s Maintenance and Support Schedule, as appended as Exhibit 1 to this **Schedule B**.

“Technical Specification” means, with respect to any Software, the document setting forth the technical specifications for such Software and included in the Statement of Work.

“Testing Period” has the meaning set forth in **Section 4.2(b)**.

“User Data” means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, processed, generated or output by any device, system or network by or on behalf of the State, including any and all data, analyses and other information and materials resulting from any use of the Software by or on behalf of the State under this Contract, except that User Data does not include the Software or data, information or content, including any GUI, audio, visual or digital or other display or output, that is generated automatically upon executing the Software without additional user input.

“Warranty Period” means the ninety (90) calendar-day period commencing on the date of the State’s Acceptance of the Software.

2. License Grant and Restrictions.

2.1 Software License for Software Hosted On-site. Contractor hereby grants to the State and its Authorized Users the right and license to use the Software and Documentation in accordance with the terms and conditions of this Contract and the License Agreement set forth in **Schedule D** (the “License Agreement”).

2.2 Use. The State will pay Contractor the corresponding Fees set forth in **Schedule B – Pricing and Fees**, for all Authorized Users access and use of the Software. Such Fees will be Contractor’s sole and exclusive remedy for any excessive use of the Software.

2.3 Open-Source Licenses. Any use hereunder of Open-Source Components shall be governed by, and subject to, the terms and conditions of the applicable opensource license (“Open-Source License”). Contractor shall identify and describe in an exhibit to the Statement of Work each of the Approved Open-Source Components of the Software, and include an exhibit attaching all applicable Open-Source Software Licenses or identifying the URL where these licenses are publicly available.



3. Software Implementation.

- 3.1 Implementation. Contractor will deliver, install, configure, integrate, and otherwise provide and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the criteria set forth in the Statement of Work.
- 3.2 Site Preparation. Unless otherwise set forth in the Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to deliver and install the Software on or prior to the applicable Milestone Date. Contractor will provide the State with such notice as is specified in the Statement of Work, prior to delivery of the Software to give the State sufficient time to prepare for Contractor's delivery and installation of the Software. If the State is responsible for Site preparation, Contractor will provide such assistance as the State requests to complete such preparation on a timely basis.

4. Testing and Acceptance.

- 4.1 Pre-Delivery Testing by Contractor. Before delivering and installing the Software, Contractor must:
- (a) test the Software to confirm that it is fully operable, meets all applicable Specifications and will function in accordance with the Specifications and Documentation when properly installed in the Operating Environment;
 - (b) scan the Software using industry standard scanning software and definitions to confirm it is free of Harmful Code; and
 - (c) remedy any Non-Conformity or Harmful Code identified and retest and rescan the Software.
- 4.2 Acceptance Testing.
- (a) Unless otherwise specified in the Statement of Work, upon installation of the Software, Acceptance Tests will be conducted to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation.
 - (b) All Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in the Statement of Work, commence on the Business Day following installation of the Software and be conducted diligently for up to thirty (30) Business Days, or such other period as may be set forth in the Statement of Work (the "**Testing Period**"). Acceptance Tests will be conducted by the party responsible as set forth in the



Statement of Work or, if the Statement of Work does not specify, the State, provided that:

- (i) for Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and
- (ii) for Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such Acceptance Tests.

Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of Acceptance Testing.

- (c) Upon delivery and installation of any API, Configuration or Customization to the Software under the Statement of Work, additional Acceptance Tests will be performed on the modified Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software ("**Integration Testing**"). Integration Testing is subject to all procedural and other terms and conditions set forth in **Section 4**.
- (d) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material NonConformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within ten (10) Business Days, correct such Non-Conformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period. If the material Non-Conformity cannot be corrected or fixed, then Contractor will provide substitute Software that is functionally equivalent or better, or as an option of last resort (only if the first two options are not commercially reasonable), remove the Software and refund the State.

4.3 Notices of Completion, Non-Conformities, and Acceptance. Within fifteen (15) Business Days following the completion of any Acceptance Tests, including any Integration Testing, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected NonConformity in the tested Software.

- (a) If such notice is provided by either party and identifies any NonConformities, the parties' rights, remedies, and obligations will be as set forth in **Section 4.4** and **Section 4.5**.



- (b) If such notice is provided by the State, is signed by the State's Business Owner and Program Manager, and identifies no Non-Conformities, such notice constitutes the State's Acceptance of such Software.
- (c) If such notice is provided by Contractor and identifies no Non-Conformities, the State will have thirty (30) Business Days to use the Software in the Operating Environment and determine that the Software contains no NonConformities, on the completion of which the State will, as appropriate:
 - (i) notify Contractor in writing of Non-Conformities the State has observed in the Software and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Section 4.4** and **Section 4.5**; or
 - (ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State's Business Owner and Program Manager.

4.4 Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Non-Conformities and re-deliver the Software, in accordance with the requirements set forth in the Statement of Work. Redelivery will occur as promptly as commercially possible and, in any case, within thirty (30) Business Days following, as applicable, Contractor's:

- (a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or
- (b) receipt of the State's notice under **Section 4.2(a)** or **Section 4.3(c)(i)**, identifying any Non-Conformities.

4.5 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any NonConformity in the Software after a second or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

- (a) continue the process set forth in **Section 4.2**;
- (b) accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or
- (c) deem the failure to be a non-curable material breach of this Contract and the Statement of Work and terminate this Contract for cause in accordance with **Section 29** of the Contract Terms.



4.6 Acceptance. Acceptance (“**Acceptance**”) of the Software (subject, where applicable, to the State’s right to Integration Testing) will occur on the date that is the earliest of the State’s delivery of a notice accepting the Software under **Section 4.3(b)**, or **Section 4.3(c)(ii)**.

5. Training. Contractor shall provide training on all uses of the Software permitted hereunder in accordance with the times, locations and other terms set forth in the Statement of Work. Upon the State’s request, Contractor shall timely provide training for additional Authorized Users or other additional training on all uses of the Software for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

6. Support Services; Maintenance Releases; New Versions.

6.1 Support Services for On-Premise Software. If the Operating Environment for the Software is internally hosted by the State, Contractor shall provide the State with the Support Services described in the Maintenance and Support Schedule attached as **Exhibit 1** to this **Schedule B**. Such Support Services shall be provided:

- (a) Free of charge during the Warranty Period, it being acknowledged and agreed that the License Fee includes full consideration for such Services during such period.
- (b) Thereafter, for so long as the State elects to receive Support Services for the Software, in consideration of the State’s payment of Support Services Fees in accordance with the rates set forth in the Pricing Schedule.

6.2 Maintenance Releases. Provided that the State is current on its Support Services Fees, during the Term, Contractor shall provide the State, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

6.3 New Versions. Provided that the State is current on its Support Services Fees, during the Term, Contractor shall provide the State, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

6.4 EXCLUDED SERVICES.

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.



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.

7. Software Representations and Warranties.

7.1 Contractor further represents and warrants to the State that:

- (a) it is the legal and beneficial owner of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto;
- (b) it has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license hereunder;
- (c) the Software, and the State's use thereof, is and throughout the license term will be free and clear of all encumbrances, liens and security interests of any kind;
- (d) neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time:
 - (i) conflict with or violate any applicable law;
 - (ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or
 - (iii) require the provision of any payment or other consideration to any third party by the State;
- (e) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software or Documentation as delivered or installed by Contractor does not or will not:
 - (i) fail to comply with any applicable law;
- (f) as provided by Contractor, the Software does not or will not at any time during the license term contain any:
 - (i) Harmful Code; or



- (ii) Open-Source Components or operate in such a way that it is developed or compiled with or linked to any Open-Source Components, other than Approved Open-Source Components specifically described in the Statement of Work.
- (g) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the license term will the Software have any material undocumented feature; and
- (h) it will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.
- (i) when used in the Operating Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract and the Documentation; and
- (j) no Maintenance Release or New Version, when properly installed in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.

7.2 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS CONTRACT.



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

**SCHEDULE D
SOFTWARE LICENSE AGREEMENT FOR ON-SITE HOSTING**

Section 1 DEFINITIONS that apply to this Schedule D

1.1 "Designated Products" means products provided by Motorola to Licensee with which or for which the Software and Documentation is licensed for use.

1.2 "Documentation" means product and software documentation that specifies technical and performance features and capabilities, and the user, operation and training manuals for the Software (including all physical or electronic media upon which such information is provided).

1.3 "Open Source Software" means software with either freely obtainable source code, license for modification, or permission for free distribution.

1.4 "Open Source Software License" means the terms or conditions under which the Open Source Software is licensed.

1.5 "Primary Agreement" means the agreement to which this schedule is attached.

1.6 "Security Vulnerability" means a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach such that data is compromised, manipulated or stolen or the system damaged.

1.7 "Software" (i) means proprietary software in object code format, and adaptations, translations, de-compilations, disassemblies, emulations, or derivative works of such software; (ii) means any modifications, enhancements, new versions and new releases of the software provided by Motorola; and (iii) may contain one or more items of software owned by a third party supplier. The term "Software" does not include any third-party software provided under separate license or third-party software not licensable under the terms of this Schedule.



Section 2 SCOPE

Motorola and Licensee enter into this Schedule in connection with Motorola's delivery of certain proprietary Software or products containing embedded or pre-loaded proprietary Software, or both. This Schedule contains the terms and conditions of the license Motorola is providing to Licensee, and Licensee's use of the Software and Documentation.

Section 3 GRANT OF LICENSE

3.1. Subject to the provisions of this Schedule and the payment of applicable license fees, Motorola grants to Licensee a personal, limited, non-transferable (except as permitted in Section 7) and non-exclusive license under Motorola's copyrights and Confidential Information (as defined in the Primary Agreement) embodied in the Software to use the Software, in object code form, and the Documentation solely in connection with Licensee's use of the Designated Products. This Schedule does not grant any rights to source code.

3.2. If the Software licensed under this Schedule contains or is derived from Open Source Software, the terms and conditions governing the use of such Open Source Software are in the Open Source Software

Licenses of the copyright owner and not this Schedule. If there is a conflict between the terms and conditions of this Schedule and the terms and conditions of the Open Source Software Licenses governing Licensee's use of the Open Source Software, the terms and conditions of the license grant of the applicable Open Source Software Licenses will take precedence over the license grants in this Schedule. If requested by Licensee, Motorola will use commercially reasonable efforts to: (i) determine whether any Open Source Software is provided under this Schedule; (ii) identify the Open Source Software and provide Licensee a copy of the applicable Open Source Software License (or specify where that license may be found); and, (iii) provide Licensee a copy of the Open Source Software source code, without charge, if it is publicly available (although distribution fees may be applicable).

Section 4 LIMITATIONS ON USE

4.1. Licensee may use the Software only for Licensee's internal business purposes and only in accordance with the Documentation. Any other use of the Software is strictly prohibited.



4.2. Licensee will not, and will not allow or enable any third party to: (i) reverse engineer, disassemble, peel components, decompile, reprogram or otherwise reduce the Software or any portion to a human perceptible form or otherwise attempt to recreate the source code; (ii) modify, adapt, create derivative works of, or merge the Software; (iii) copy, reproduce, distribute, lend, or lease the Software or Documentation to any third party, grant any sublicense or other rights in the Software or Documentation to any third party, or take any action that would cause the Software or Documentation to be placed in the public domain; (iv) remove, or in any way alter or obscure, any copyright notice or other notice of Motorola's proprietary rights; (v) provide, copy, transmit, disclose, divulge or make the Software or Documentation available to, or permit the use of the Software by any third party or on any machine except as expressly authorized by this Schedule; or (vi) use, or permit the use of, the Software in a manner that would result in the production of a copy of the Software solely by activating a machine containing the Software. Licensee may make one copy of Software to be used solely for archival, back-up, or disaster recovery purposes; *provided* that Licensee may not operate that copy of the Software at the same time as the original Software is being operated. Licensee may make as many copies of the Documentation as it may reasonably require for the internal use of the Software.

4.3. Unless otherwise authorized by Motorola in writing, Licensee will not, and will not enable or allow any third party to: (i) install a licensed copy of the Software on more than one unit of a Designated Product; or (ii) copy onto or transfer Software installed in one unit of a Designated Product onto one other device. Licensee may temporarily transfer

Software installed on a Designated Product to another device if the Designated Product is inoperable or malfunctioning, if Licensee provides written notice to Motorola of the temporary transfer and identifies the device on which the Software is transferred. Temporary transfer of the Software to another device must be discontinued when the original Designated Product is returned to operation and the Software must be removed from the other device. Licensee must provide prompt written notice to Motorola at the time temporary transfer is discontinued.

4.4. When using Motorola's Radio Service Software ("RSS"), Licensee must purchase a separate license for each location at which Licensee uses RSS. Licensee's use of RSS at a licensed location does not entitle Licensee to use or access RSS remotely. Licensee may make one copy of RSS for each licensed location. Licensee shall provide Motorola with a list of all locations at which Licensee uses or intends to use RSS upon Motorola's request.

4.5. Licensee will maintain, during the term of this Schedule and for a period of two years thereafter, accurate records relating to this license grant to verify compliance with this Schedule. Within thirty (30) days of Contractor's request, but no more than once per year, the State shall provide a written certification of its



compliance with the terms of this Agreement. Payment to correct any non-compliances related to an audit finding shall be Contractor's sole and exclusive remedy to cure audit compliance issues.

Section 5 OWNERSHIP AND TITLE

Motorola, its licensors, and its suppliers retain all of their proprietary rights in any form in and to the Software and Documentation, including, but not limited to, all rights in patents, patent applications, inventions, copyrights, trademarks, trade secrets, trade names, and other proprietary rights in or relating to the Software and Documentation (including any corrections, bug fixes, enhancements, updates, modifications, adaptations, translations, de-compilations, disassemblies, emulations to or derivative works from the Software or Documentation, whether made by Motorola or another party, or any improvements that result from Motorola's processes or, provision of information services). No rights are granted to Licensee under this Schedule by implication, estoppel or otherwise, except for those rights which are expressly granted to Licensee in this Schedule. All intellectual property developed, originated, or prepared by Motorola in connection with providing the Software, Designated Products, Documentation or related services, remains vested exclusively in Motorola, and Licensee will not have any shared development or other intellectual property rights.

Section 6 LIMITED WARRANTY; DISCLAIMER OF WARRANTY

6.1. The commencement date and the term of the Software warranty will be a period of ninety (90) days from Motorola's shipment of the Software (the "Warranty Period"). If Licensee is not in breach of any of its obligations under this Schedule, Motorola warrants that the unmodified Software, when used properly and in accordance with the Documentation and this Schedule, will be free from a reproducible defect that eliminates the functionality or successful operation of a feature critical to the primary functionality or successful operation of the Software. Whether a defect occurs will be determined by Motorola solely with reference to the Documentation. Motorola does not warrant that Licensee's use of the Software or the Designated Products will be uninterrupted, error-free, completely free of Security Vulnerabilities, or that the Software or the Designated Products will meet Licensee's particular requirements. Motorola makes no representations or warranties with respect to any third-party software included in the Software.

6.2 Licensee's exclusive remedy under this warranty (in conjunction with the State's right to terminate this Contract for breach, where applicable, and any remedy set forth in the Service Level Agreement) is to use reasonable efforts to remedy any material Software defect covered by this warranty. These efforts will involve either replacing the media or attempting to correct significant,



demonstrable program or documentation errors or Security Vulnerabilities. If Motorola cannot correct the defect within a reasonable time, then at Motorola's option, Motorola will replace the defective Software with functionally equivalent Software, license to Licensee substitute Software which will accomplish the same objective or terminate the license and refund the Licensee's paid license fee.

6.3. Warranty claims are described in the Primary Agreement.

6.4. The express warranties set forth in this Section 6 are in lieu of, and Motorola disclaims, any and all other warranties (express or implied, oral or written) with respect to the Software or Documentation, including, without limitation, any and all implied warranties of condition, title, merchantability, or fitness for a particular purpose or use by Licensee (whether or not Motorola knows, has reason to know, has been advised, or is otherwise aware of any such purpose or use), whether arising by law, by reason of custom or usage of trade, or by course of dealing. In addition, Motorola disclaims any warranty to any person other than Licensee with respect to the Software or Documentation.

Section 7 TRANSFERS

Licensee will not transfer the Software or Documentation to any third party without Motorola's prior written consent. Motorola's consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this Schedule. If the Designated Products are Motorola's radio products and Licensee transfers ownership of the Motorola radio products to a third party, Licensee may assign its right to use the Software (other than RSS and Motorola's FLASHport® software) which is embedded in or furnished for use with the radio products and the related Documentation; *provided* that Licensee transfers all copies of the Software and Documentation to the transferee, and Licensee and the transferee sign a transfer form to be provided by Motorola upon request, obligating the transferee to be bound by this Schedule.

Section 8 TERM

8.1 Licensee's right to use the Software and Documentation will begin when the Primary Agreement is signed by both parties and will continue for the life of the Designated Products with which or for which the Software and Documentation have been provided by Motorola unless Licensee breaches Section 4.1, 4.2, or 4.3 of this Agreement, in which case this Agreement and Licensee's right to use the Software and Documentation may be terminated after written notice from Motorola and the Licensee's failure to cure such breach within seven (7) business days of its receipt of the written notice.

**Section 9 GENERAL**

9.1 COPYRIGHT NOTICES. The existence of a copyright notice on the Software will not be construed as an admission or presumption of publication of the Software or public disclosure of any trade secrets associated with the Software.

9.2 SECURITY. Motorola uses reasonable means in the design and writing of its own Software and the acquisition of third-party Software to limit Security Vulnerabilities. While no software can be guaranteed to be free from Security Vulnerabilities, if a Security Vulnerability is discovered, Motorola will take the steps set forth in Section 6 of this Agreement.



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

SCHEDULE E- SOFTWARE SUPPORT POLICY

This document defines specific support availability and timelines for Motorola Solutions ASTRO® 25 and Dimetra systems.

Support Periods: The standard support period begins when a system software release is first made available to the market. From that date, the standard support period for the software release is four years, referred to as Year 1 to Year 4 or Y1 to Y4. The extended support period is from year 5 to year 7 or Y5 to Y7. Depending on the support option, the End of Support (EoS) period is from either year 5 or year 8 and into the future. These support periods are not affected by the purchase date, shipment date or acceptance date of a system for a given software release.

A. **Standard support period:** Motorola Solutions will support the given software release in the following manner:

1. Support Service Availability

- a. Period: Y1 through Y4 from initial market availability of the software release
- b. All Support Services available

2. Software Defect Repair / Patching

- a. Period: Y1 through Y2
- b. Qualified Severity 1 and Severity 2 incidents that result in product defect fixes will be made available to the customer. Some defects may require an upgrade to a more current release to resolve.
- c. Period: Y3 through Y4
- d. Qualified Severity 1 incidents that result in product defect fixes will be made available to the customer. Some defects may require an upgrade to a more current release to resolve.

3. Security Services

- a. Period: Y1 through Y4
- b. All Security Services available (Security Monitoring and Security Update Service)

4. System Expansion

- a. Period: Y1 through Y4



- b. Full system expansion available including subscribers, sites, consoles, base stations and radio system Customer Enterprise Network (CEN) additions.

B. Extended Support Period: Applies to software releases that have reached the end of Standard Support. Motorola Solutions continues to provide support on such products as specified below. Extended Support includes:

1. Support Service Availability

- a. Period: Y5 through Y7
- b. All Support Services available through pricing of these services will be escalated.

2. Software Defect Repair / Patching

- a. Period: Y5 through Y7
- b. Defect Repair: Not available

3. Security Services

- a. Period: Y5 through Y7
- b. Security Services - Not available

4. System Expansion

- a. Period: Y5 through Y7
- b. Infrastructure expansions are not available. System Expansion is limited to subscribers only. Some features on the subscribers may not function due to Infrastructure expansions no longer being available.

C. End of Support Period: Applies to software releases that have reached the end of Extended Support. Support for older software versions will no longer be available. End of Support includes:

1. Support Service Availability and Pricing

- a. Period: Y8 and later
- b. Support Services - Not Available

2. Software Patching

- a. Period: Y5 and later
- b. Defect Repair - Not Available
- c. Security Services - Not Available

3. System Expansion

- a. Period: Y5 and later
- b. Infrastructure expansions are not available. System Expansion is limited to subscribers only. Some features on the subscribers may not function due to Infrastructure expansions no longer being available.



Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

SCHEDULE F Federal Provisions Addendum

The provisions in this addendum may apply if the purchase will be paid for in whole or in part with funds obtained from the federal government. If any provision below is not required by federal law for this Contract, then it does not apply and must be disregarded. If any provision below is required to be included in this Contract by federal law, then the applicable provision applies, and the language is not negotiable. If any provision below conflicts with the State's terms and conditions, including any attachments, schedules, or exhibits to the State's Contract, the provisions below take priority to the extent a provision is required by federal law; otherwise, the order of precedence set forth in the Contract applies. Hyperlinks are provided for convenience only; broken hyperlinks will not relieve Contractor from compliance with the law.

1. **Federally Assisted Construction Contracts.** If this contract is a “**federally assisted construction contract**” as defined in [41 CRF Part 60-1.3](#), and except as otherwise may be provided under [41 CRF Part 60](#), then during performance of this Contract, the Contractor agrees as follows:
 - (1) The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following: Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.
 - (2) The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.
 - (3) The Contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to



instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the Contractor's legal duty to furnish information.

(4) The Contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the Contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(5) The Contractor will comply with all provisions of [Executive Order 11246](#) of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

(6) The Contractor will furnish all information and reports required by [Executive Order 11246](#) of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

In the event of the Contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this Contract may be canceled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in [Executive Order 11246](#) of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in [Executive Order 11246](#) of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(7) The Contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of [Executive Order 11246](#) of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:

Provided, however, that in the event a Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the



administering agency, the Contractor may request the United States to enter into such litigation to protect the interests of the United States.

2. Davis-Bacon Act (Prevailing Wage)

- a. If applicable, the Contractor (and its Subcontractors) for **prime construction contracts** in excess of \$2,000 must comply with the Davis-Bacon Act ([40 USC 3141-3148](#)) as supplemented by Department of Labor regulations ([29 CFR Part 5](#), “Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction”).
- b. The Contractor (and its Subcontractors) shall pay all mechanics and laborers employed directly on the site of the work, unconditionally and at least once a week, and without subsequent deduction or rebate on any account, the full amounts accrued at time of payment, computed at wage rates not less than those stated in the advertised specifications, regardless of any contractual relationship which may be alleged to exist between the Contractor or subcontractor and the laborers and mechanics;
- c. The Contractor will post the scale of wages to be paid in a prominent and easily accessible place at the site of the work;
- d. There may be withheld from the Contractor so much of accrued payments as the contracting officer considers necessary to pay to laborers and mechanics employed by the Contractor or any Subcontractor on the work the difference between the rates of wages required by the Contract to be paid laborers and mechanics on the work and the rates of wages received by the laborers and mechanics and not refunded to the Contractor or Subcontractors or their agents.

3. Copeland “Anti-Kickback” Act. If applicable, the Contractor must comply with the [Copeland “Anti-Kickback” Act \(40 USC 3145\)](#), as supplemented by Department of Labor regulations ([29 CFR Part 3](#), “Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States”), which prohibits the Contractor and subrecipients from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled.

4. **Contract Work Hours and Safety Standards Act.** If the Contract is **in excess of \$100,000 and involves the employment of mechanics or laborers**, the Contractor must comply with [40 USC 3702](#) and [3704](#), as supplemented by Department of Labor regulations ([29 CFR Part 5](#)), as applicable.
5. **Rights to Inventions Made Under a Contract or Agreement.** If the Contract is funded by a federal “funding agreement” as defined under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that “funding agreement,” the recipient or subrecipient must comply with 37 CFR Part



401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

6. **Clean Air Act.** If this Contract is **in excess of \$150,000**, the Contractor must comply with all applicable standards, orders, and regulations issued under the Clean Air Act (42 USC 7401-7671q) and the Federal Water Pollution Control Act (33 USC 1251-1387). Violations must be reported to the federal awarding agency and the regional office of the Environmental Protection Agency.
7. **Debarment and Suspension.** A "contract award" (see [2 CFR 180.220](#)) must not be made to parties listed on the government-wide exclusions in the [System for Award Management](#) (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.
8. **Byrd Anti-Lobbying Amendment.** If this Contract **exceeds \$100,000**, Contractors and the Contractor must file the certification required under [31 USC 1352](#).
9. **Procurement of Recovered Materials.** Under [2 CFR 200.322](#), a non-Federal entity that is a state agency or agency of a political subdivision of a state **and its contractors** must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at [40 CFR part 247](#) that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

Byrd Anti-Lobbying Certification

The following certification and disclosure regarding payments to influence certain federal transactions are made under FAR 52.203-11 and 52.203-12 and [31 USC 1352](#), the "Byrd Anti-Lobbying Amendment." Hyperlinks are provided for convenience only; broken hyperlinks will not relieve Contractor from compliance with the law.

1. [FAR 52.203-12](#), "Limitation on Payments to Influence Certain Federal Transactions" is hereby incorporated by reference into this certification.
2. The Contractor, by submitting its proposal, hereby certifies to the best of his or her knowledge and belief that:
 - a. No federal **appropriated** funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress,



- or an employee of a member of Congress on his or her behalf in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment or modification of any federal contract, grant, loan, or cooperative agreement;
- b. If any funds **other than federal appropriated funds** (including profit or fee received under a covered federal transaction) have been paid, or will be paid, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress on his or her behalf **in connection with this solicitation**, the Contractor must complete and submit, with its proposal, [OMB standard form LLL, Disclosure of Lobbying Activities](#), to the Solicitation Manager; and
 - c. He or she will include the language of this certification in all subcontract awards at any tier and require that all recipients of subcontract awards in excess of \$150,000 must certify and disclose accordingly.
3. This certification is a material representation of fact upon which reliance is placed at the time of Contract award. Submission of this certification and disclosure is a prerequisite for making or entering into this Contract under [31 USC 1352](#). Any person making an expenditure prohibited under this provision or who fails to file or amend the disclosure form to be filed or amended by this provision is subject to a civil penalty of not less than \$10,000, and not more than \$100,000, for each such failure.

Signed by:

Robert Rummel, Motorola Solutions Sales & Services Inc. Vice President
Motorola Solutions Inc.

Date: _____

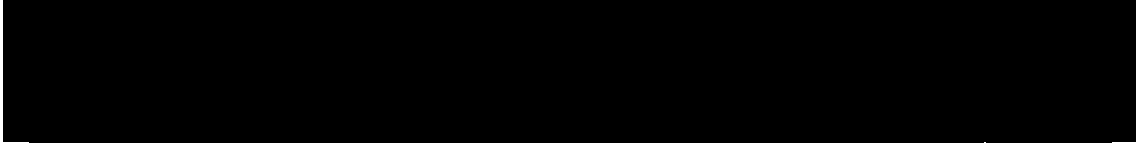


Michigan's Public Safety Communications System (MPSCS) Continued System Updates, Equipment Maintenance and Upgrades, and Ancillary Systems Products

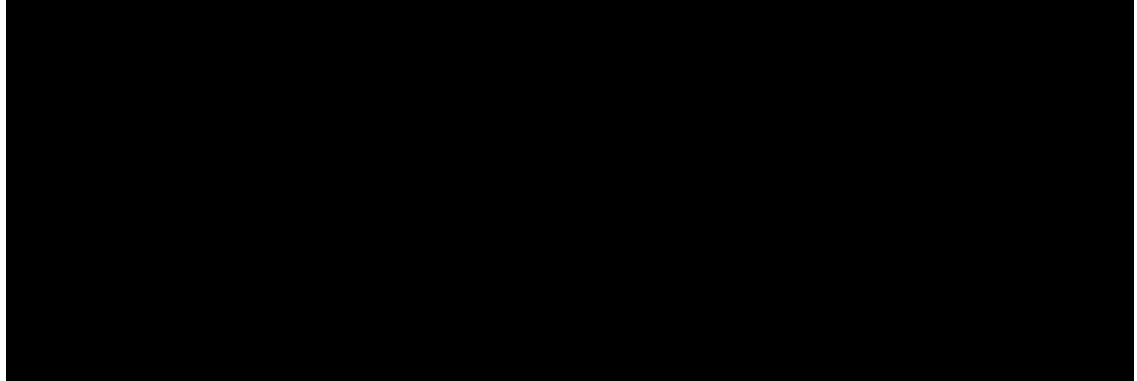
**SCHEDULE G
System Configuration**

System at Contract Initiation Including Contracted/Anticipated Integrations through 2025

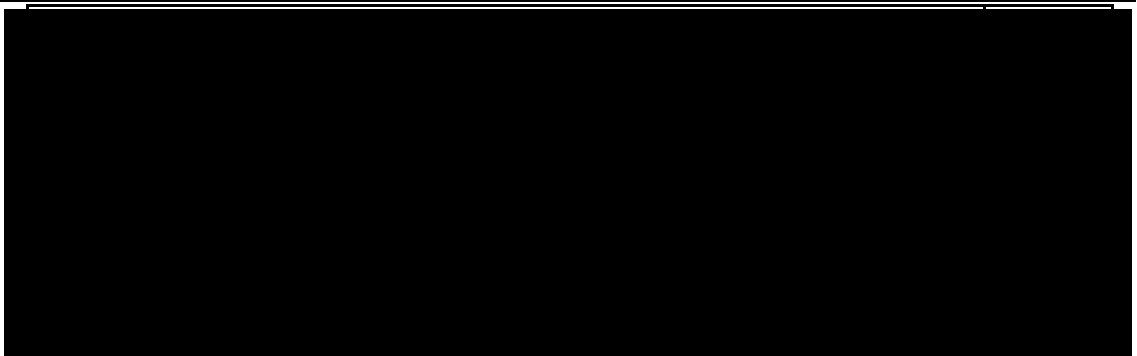
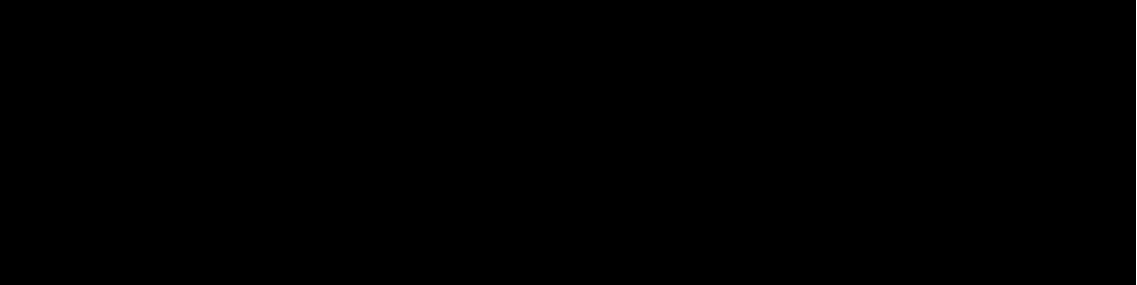
Master Site Configuration	
---------------------------	--



System Level Features	
-----------------------	--



Security Configuration	
------------------------	--





Dispatch Site Configuration

[Redacted Content]	[Redacted Content]
--------------------	--------------------

Third Party Elements[g2]

[Redacted Content]	[Redacted Content]
--------------------	--------------------



Contracted Integrations Scheduled for 10/1/19 through 12/31/2025 with Scope Defined by the Final Accepted Detailed Design Plan as of 10/1/19

ENTITY
Branch
Calhoun County
CCE
Dearborn
Detroit
Eaton County
Ingham County
Iosco County
Jackson County
Kent County
Lenawee County
MPSCS NCC Logging
MSU RCM
Muskegon County
NCC Backup
Newago County
Northville Township
Oakland County
Ottawa Site
Saginaw Chippewa
St. Clair County
St. Joseph County
Wolverine Power
University of Michigan