RESOLUTION NO. 2024 - 286

A RESOLUTION BY THE BOARD OF COUNTY COMMISSIONERS OF ST. JOHNS COUNTY, FLORIDA, AUTHORIZING THE COUNTY ADMINISTRATOR, OR DESIGNEE, TO EXECUTE SINGLE SOURCE SS 1680; CYBER SECURITY FOR CAD RADIO SYSTEM WITH MOTOROLA SOLUTIONS, INC., AND AWARD AND EXECUTE A CONTRACT FOR CYBER SECURITY THAT MANAGES DETECTIONS AND HANDLES RESPONSES.

RECITALS

WHEREAS, the County requires cyber security for the St. Johns County Fire Rescue Department and the St. Johns County Communications Department, as specified, in accordance with SS 1680; and

WHEREAS, SJC Purchasing posted a single source notice in accordance with policy and Florida Statutes, and received no additional responses from firms to provide the specified services; and

WHEREAS, the Fire Rescue Department and the Communications Department need to add ASTRO25 Managed Detection and Response Cyber Security, which provides testing for vulnerabilities of our networks, servers, interfaces with partner entities, and other network components to ensure protection and mitigation for corruption, in the amount of $668,694.31, for (5) five years for ASTRO25 Managed Detection and Response; and

WHEREAS, the contract will be in substantial conformance with the attached draft; and

WHEREAS, the County has reviewed the terms, provisions, conditions and requirements of the proposed amendment (attached hereto, and incorporated herein) and finds that executing the amendment to complete the Cyber Security additions; and,

NOW, THEREFORE BE IT RESOLVED BY THE BOARD OF COUNTY COMMISSIONERS OF ST. JOHNS COUNTY, FLORIDA, as follows:

Section 1. The above Recitals are incorporated by reference into the body of this Resolution and such Recitals are adopted as finds of fact.

Section 2. The County Administrator, or designee, is hereby authorized to award and execute a contract in substantially the same form and format as attached with Motorola Solutions, Inc., to provide Cyber Security for a not-to-exceed amount of $668,694.31.

Section 4. To the extent that there are typographical and/or administrative errors that do not change the tone, tenor, or concept of this Resolution, then this Resolution may be revised without subsequent approval by the Board of County Commissioners.

PASSED AND ADOPTED by the Board of County Commissioners of St. Johns County, Florida, on this 16th day of July, 2024.

Rendition Date JUL 16 2024

BOARD OF COUNTY COMMISSIONERS OF ST. JOHNS COUNTY, FLORIDA

By: _____
Sarah Arnold, Chair

ATTEST: Brandon J. Patty,
Clerk of the Circuit Court & Comptroller

By: Crystal Smith
Deputy Clerk

ST. JOHNS COUNTY FLORIDA

Firm Fixed Price Proposal

St. John's County Board of Commissioners

ASTRO 25 Managed Detection and Response

24-175960 / Cybersecurity Services

July 1, 2024

The design, technical, and price information furnished with this proposal is proprietary information of Motorola Solutions, Inc. (Motorola). Such information is submitted with the restriction that it is to be used only for the evaluation of the proposal, and is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the proposal, without the express written permission of Motorola Solutions, Inc.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2024 Motorola Solutions, Inc. All rights reserved.

PS-000175960

Table of Contents

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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

July 1, 2024

Lee Mathis
LMR Manager
500 San Sebastian View
St. Augustine, FL 32084

RE: ASTRO® Managed Detection and Response

Dear Mr. Mathis:

Motorola Solutions, Inc. (Motorola) appreciates the opportunity to provide St. John's County Board of Commissioners quality cybersecurity equipment and services. Motorola's project team has taken great care to propose a solution to address your needs and provide exceptional value.

Motorola's proposal is conditional upon St. John's County Board of Commissioners' acceptance of the terms and conditions included in this proposal, or a negotiated version thereof. Pricing will remain valid for ninety (90) days.

Any questions St. John's County Board of Commissioners has regarding this proposal can be directed to Jim Feild, Cybersecurity Account Manager at 443-478-6995 or by email at james.feild@motorolasolutions.com.

Our goal is to provide St. John's County Board of Commissioners with the best products and services available in the cybersecurity industry. We thank you for the opportunity to present our proposed solution, and we hope to strengthen our relationship by implementing this project.

Sincerely,

Mike Allen
Area Sales Manager, Cybersecurity – North America
MOTOROLA SOLUTIONS, INC.

Section 1

Executive Summary

Motorola is pleased to build upon our years of ongoing support to St. John's County Board of Commissioners with a proposal that efficiently meets the needs for your ASTRO® 25 Managed Detection and Response (MDR) solution. We are a national and global leader in the cybersecurity community with our recent acquisitions of both Delta Risk and Lunarline in 2020. We have evolved into a holistic mission critical technology provider, placing Information Technology (IT), as well as cybersecurity, at the forefront of importance to protect our customers against threats to the confidentiality, integrity and availability of their operation.

ASTRO 25 Managed Detection and Response

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

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

The ActiveEye℠ Platform

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

- **Included Public Safety Threat Data Feed** — Threat reports covering potential attack vectors based on dark web research. Summaries of actual attacks against public safety and state/local municipalities. Indicator data pulled from a large network of deployed public safety sensors and state/local municipality environments.
- **Advanced Threat Detection & Response** — Consolidate SIEM data and direct threat inputs from endpoint security, network sensors, and cloud/SaaS applications. Pre-built custom playbooks to process alerts and reduce/eliminate manual analyst effort.
- **Single Dashboard for Threat Visibility** — Prioritize based on actual assets in the environment. Asset inventory created manually or automatically with Managed Vulnerability Assessment Service - external and authenticated scans of assets, providing a complete attack surface map.

Chief Information Security Officer (CISO) Benefits

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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

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

Public Safety Threat Alliance

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

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

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

ABOUT MOTOROLA

Company Background and History

Motorola creates innovative, mission-critical communication solutions and services that help public safety and commercial customers build safer cities and thriving communities. You can find our products at work in a variety of industries including law enforcement, fire, emergency medical services, national government security, utilities, mining, energy, manufacturing, hospitality, retail, transportation and logistics, education, and public services. Our communication solutions span infrastructure, devices, services and software to help our public safety and commercial customers be more effective and efficient.

Company Overview

Since 1928, Motorola Solutions, Inc. (formerly Motorola, Inc.) has been committed to innovation in communications and electronics. Our company has achieved many milestones in its history. We pioneered mobile communications in the 1930s with car radios and public safety networks. We made the equipment that carried the first words from the moon in 1969. We commercialized the first handheld portable scanner in 1980. Today, as a global industry leader, excellence in innovation continues to shape the future of the Motorola brand.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

We help people be their best in the moments that matter.

Motorola connects people through technology. Public safety and commercial customers around the world turn to Motorola innovations when they want highly connected teams that have the information they need throughout their workdays and in the moments that matter most to them.

Our customers rely on us for the expertise, services, and solutions we provide, trusting our years of invention and innovation experience. By partnering with customers and observing how our products can help in their specific industries, we are able to enhance our customers' experience every day.

Motorola's Corporate Headquarters is located at 500 West Monroe Street, Chicago, IL 60661. Telephone is +1 847.576.5000, and the website is www.motorolasolutions.com.

Section 2

Solution Description

2.1 Solution Overview

Motorola Solutions, Inc. (Motorola) is pleased to present the proposed cybersecurity Managed Detection and Response (MDR) services for St. John's County Board of Commissioners (hereinafter referred to as "Customer").

Identifying and mitigating cyber threats requires a reliable solution that supplies the right data to cybersecurity experts. 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 in our proposal:

- **ActiveEye℠ Managed Detection and Response Elements**
  - ActiveEye℠ Security Management Platform
  - ActiveEye℠ Remote Security Sensor (AERSS)
- **Service Modules**
  - Log Collection / Analytics
  - Network Detection
  - Attack Surface Management
- **Security Operations Center Monitoring and Support**

2.1.1 Site Information

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

Table 2-1: Site Information

Site / Location	Quantity
Core Site	1
Control Room CEN	2
Co-located CEN	1
Network Management Clients	6
Dispatch Consoles	37
CEN Endpoints	30

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Services Included

The ActiveEye[SM] service modules included in our proposal are selected in the **Subscribed** column below. The **Network Environment** column will designate the location of each module: ASTRO 25 Radio Network Infrastructure (RNI), Customer Enterprise Network (CEN), or the Control Room CEN.

Table 2-2: Service Modules

Service Module	Features Included	Network Environment	Subscribed
ActiveEye[SM] Remote Security Sensor (AERSS)	Number of sensors: 4 (1) Core Site (3) CEN	RNI CEN	X
Log Collection / Analytics	Online Storage Period: 30 Day Storage Extended Log Storage Length: 12 Months	RNI CEN	X
Network Detection	Up to 1 Gbps per sensor port	RNI CEN	X
Attack Surface Management	Features in Section 3.2.3.3	RNI CEN	X

2.2 Service Description

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

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

The MDR service includes the deployment and optimization of these elements into the Customer's network. The Service also provides Cybersecurity awareness and best practices training to fortify the first line of defense, the organization's people. A single subscription (1 seat) to Motorola Solutions online Learning Hub for Cybersecurity is included.

2.2.1 Managed Detection and Response Elements

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

2.2.1.1 ActiveEye[SM] Security Platform

Motorola's ActiveEye[SM] security platform collects and analyzes security event streams from ActiveEye[SM] Remote Security Sensors (AERSS) in the Customer's ASTRO 25 network and applicable

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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^{SM} platform as part of this service. ActiveEye^{SM} will serve as a single interface to display system security information. Using ActiveEye^{SM}, 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.

2.2.1.2 ActiveEye^{SM} Managed Security Portal

The ActiveEye^{SM} 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.

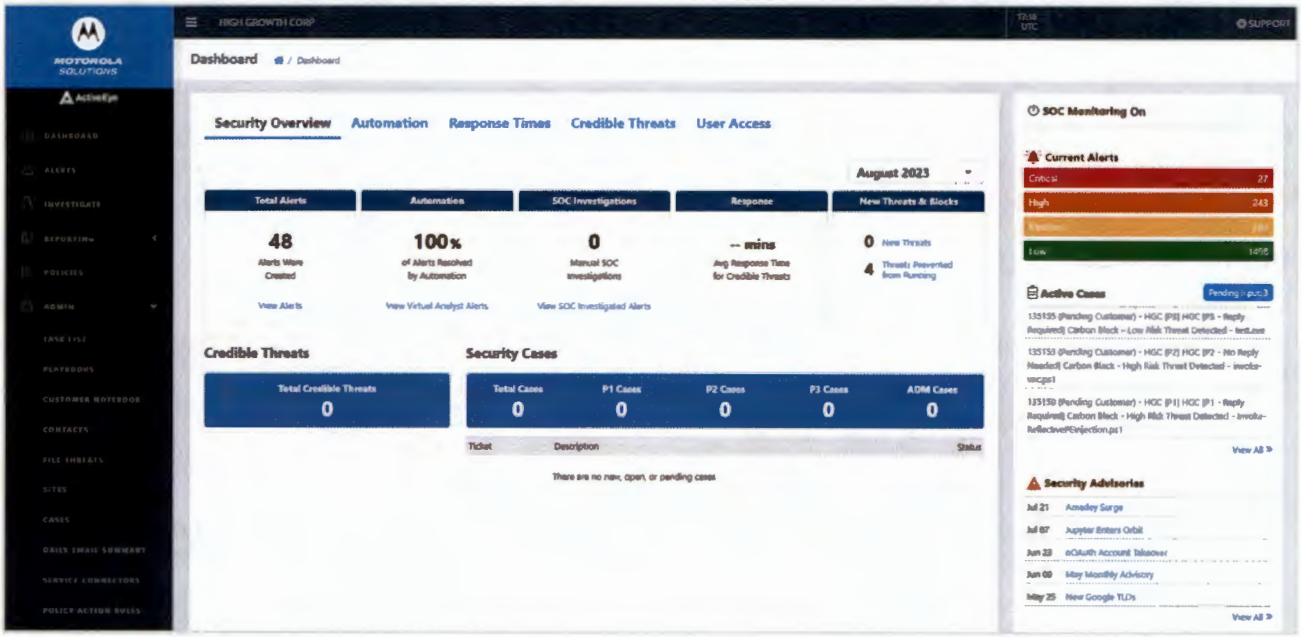

Figure 2-1: ActiveEye^{SM} Portal

Dashboard

Key information in the ActiveEye^{SM} 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 SOC will create a security case. Through the ActiveEye^{SM} Portal, the Customer can view details of current or past cases, create new cases, or respond to ongoing cases.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Alert Details and Trends

Alerts can be evidence of a past, active, or developing threat. ActiveEye[SM] 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[SM] 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[SM] 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[SM] 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[SM] Portal by downloading reports in .csv or .json format.

In addition to *ad hoc* reporting, ActiveEye[SM] 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[SM] Portal can send one or more summary emails with different content for different groups. Monthly reports are available as a PDF download.

Security Advisories

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

Information Sharing

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

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

User Access

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

2.2.1.3 ActiveEye[SM] Remote Security Sensor

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

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

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

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

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

2.2.2 Service Modules

ActiveEye[SM] delivers service capability by integrating one or more service modules. These modules provide ActiveEye[SM] 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[SM] service module in detail.

2.2.2.1 Log Collection / Analytics

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

Collected events will be stored in the ActiveEye[SM] 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 2-2: Service Modules for subscription details.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

2.2.2.2 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 SOC for further analysis.

2.2.2.3 Attack Surface Management

Attack Surface Management 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.

2.2.3 Security Operations Center Services

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Section 3

Statement of Work

3.1 Overview

In accordance with the terms and conditions of the Agreement, this Statement of Work (SOW), including all of its subsections and attachments, defines the principal activities and responsibilities of all parties for the delivery of Motorola Solutions, Inc. (Motorola) Cybersecurity services as presented in this proposal to St. John's County Board of Commissioners (Customer).

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

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

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

3.2 Description of Service

3.2.1 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 Security Operations team. The portal will enable service notifications, access to vulnerability scans and cybersecurity advisories. The first vulnerability scan will be conducted and reported within the first 30-day period. The Customer will receive instructions for accessing the Security Operations Center and Incident Response (IR) teams within the first 30 days. Once access is provisioned, the customer will receive any assistance required from the IR team. Access will also be provided to the Cybersecurity Learning portal.

Phase 2: Infrastructure Readiness

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

preparations. It is Motorola's responsibility to separately complete any obligated and/or agreed infrastructure readiness tasks.

Phase 3: System Buildout and Deployment

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

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

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

3.2.2 General Responsibilities

3.2.2.1 Motorola Responsibilities

- Provide, maintain, and when necessary, repair under warranty hardware and software required to monitor the ASTRO 25 network and applicable CEN systems Inclusive of the AERSS and all software operating on it.
  - If the Centralized Event Logging feature is not installed on the Customer's ASTRO 25 RNI, Motorola will install it as part of this service.
- Coordinate with the Customer on any system changes necessary to integrate the AERSS into the system and establish necessary connectivity.
- Provide software and licenses to the Customer necessary to remotely monitor the ASTRO 25 network and applicable CEN environments.
- Verify connectivity and monitoring is active prior to start of service.
- Coordinate with the Customer to maintain Motorola service authentication credentials.
- Monitor the Customer's ASTRO 25 network and applicable CEN systems 24/7/365 for malicious or unusual activity.
- Respond to security incidents in the Customer's system in accordance with Section 3.3.6: 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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

development or informing the Customer to enact the Customer's documented Incident Response plan.

- Assist the Customer with identifying devices that support logging within the ASTRO 25 network and applicable CEN systems have been configured to forward Syslog events to the AERSS.
- Provide the Customer with access to the ActiveEye[SM] platform enabling Customer access to security event and incident details.

3.2.2.2 Customer Responsibilities

- The ASTRO 25 MDR service requires a connection from the Customer's ASTRO 25 network and applicable CEN systems to the Internet. Establish connectivity with sufficient bandwidth before service commences. Internet service bandwidth requirements are as follows:
  - Bandwidth throughput of 10MB
  - High availability Internet Connection (99.99% (4-9s) or higher)
  - Packet loss < 0.5%
  - Jitter <10 ms
  - Delay < 120 ms
  - RJ45 Port Speed - Auto Negotiate
- Maintain an active subscription for:
  - Security Update Service (SUS) (or Remote Security Update Service), ensuring patches and antivirus definitions are applied according to the release cadence of the service.
  - ASTRO Dispatch Service and ASTRO Infrastructure Response.
- 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.
- 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.
- Provide continuous utility service(s) to any equipment installed or utilized at the Customer's premises to support service delivery and remote monitoring.
- Provide Motorola with contact information necessary to complete the Customer Support Plan (CSP). Notify the Customer's Customer Support Manager (CSM) within two weeks of any contact information changes.
- Notify Motorola 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.
- Allow Motorola's dispatched field service technicians physical access to monitoring hardware when required.
- Cooperate with Motorola and perform all acts that are required to enable Motorola to provide the services described in this SOW.
- Respond to Cybersecurity Incident Cases created by the Motorola SOC.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

3.2.3 Service Modules

The following subsections describe the delivery of the service modules selected in Table 2-2: Service Modules.

3.2.3.1 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[SM] platform, which uses advanced analytics to identify signs of security incidents. If it identifies signs of a security incident, ActiveEye[SM] notifies the SOC for further analysis.

Motorola Responsibilities

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

Customer Responsibilities

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

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

3.2.3.2 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 SOC for further analysis.

Motorola Responsibilities

- Work with the Customer to integrate AERSS.
- Optimize the policies and configuration to tune out noise and highlight potential threats.
- The SOC consults with the Customer to identify the appropriate deployment of Network Detection Service Components. The SOC 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.

Customer Responsibilities

- If necessary, configure Customer's networking infrastructure to allow AERSS to communicate with ActiveEye[SM] as defined.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- 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^{SM} sensor.
- Initiate recommended response actions when active attacks are detected.

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

3.2.3.3 Attack Surface Management

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

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

Motorola Responsibilities

- Configure scans to match the Customer's preferences for external scope.
- Verify vulnerability scans are operating correctly.
- Make generated results available in the Customer's ActiveEye^{SM} portal.
- Create ticket notifications for significant, new findings of interest.

Customer Responsibilities

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

Applies to Internet facing assets only.

3.2.4 Cybersecurity Awareness and Best Practices Training

A key component of any cybersecurity program is ensuring people involved in managing and using IT systems understand specific cybersecurity practices to both prevent actions that involuntarily create cybersecurity risk and respond quickly if a compromise is suspected. The Managed Detection and Response service provides access to an online subscription based Learning Hub, containing courses and content focused on the Cybersecurity needs of our customers. There are a number of

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Cybersecurity Modules offered through the hub via a variety of teaching methods and courses, providing timely, relevant and custom-fit cybersecurity training.

A single subscription to the Learning Hub is provided during Service Onboarding. The number of subscriptions and duration can be scaled to meet customer needs.

3.3 Security Operations Center Monitoring and Support

3.3.1 Scope

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

Motorola's SOC is staffed with security experts who will use ActiveEye^{SM} Security Management Platform to monitor elements integrated by service modules. In addition, SOC staff will take advantage of their extensive experience to investigate and triage detected threats, and to recommend responses to the Customer. 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 3.2.1: Deployment Timeline and Milestones.

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

3.3.2 Ongoing Security Operations Center Service Responsibilities

Motorola Responsibilities

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

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

Customer Responsibilities

- Provide Motorola with accurate and up-to-date information, including the name, email, landline telephone numbers, and mobile telephone numbers for all designated, authorized Customer escalation Points of Contact (PoC).
- Provide a timely response to SOC security incident tickets or investigation questions.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

3.3.3 Technical Support

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

Motorola Responsibilities

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

Customer Responsibilities

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

Limitations and Exclusions

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

3.3.4 Incident Response

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

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

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

Motorola Responsibilities

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Customer Responsibilities

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

3.3.5 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 3-1: Event Handling

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

Notification

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

Table 3-2: Notification Procedures

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

Motorola 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.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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

Tuning Period Exception

The tuning period is considered to be the first 30 days after each service module has been confirmed deployed and configured and starts receiving data. During the tuning period, Motorola 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.

3.3.6 Incident Priority Level Definitions and Response Times

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

Table 3-3: Priority Level Definitions and Response Times

Incident Priority	Incident Definition	Notification Time
Critical P1	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. Examples: • Malware that is not quarantined by anti-virus. • Evidence that a monitored component has communicated with suspected malicious actors.	Response provided 24 hours, 7 days a week, including US public holidays.
High P2	Security incidents that have localized impact, and may become more serious if not quickly addressed. Effort to recover from the incident may be moderate to significant. Examples: • Malware that is quarantined by antivirus. • Multiple behaviors observed in the system that are consistent with known attacker techniques.	Response provided 24 hours, 7 days a week, including US public holidays.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Incident Priority	Incident Definition	Notification Time
Medium P3	Security incidents that potentially indicate an attacker is performing reconnaissance or initial attempts at accessing the system. Effort to recover from the incident may be low to moderate. Examples include: • Suspected unauthorized attempts to log into user accounts. • Suspected unauthorized changes to system configurations, such as firewalls or user accounts. • Observed failures of security components. • Informational events. • User account creation or deletion. • Privilege change for existing accounts.	Response provided on standard business days, Monday through Friday 8:00 a.m. to 5:00 p.m. CST/CDT, excluding US public holidays.
Low P4	These are typically service requests from the Customer.	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.

3.3.6.1 Response Time Goals

Priority	Response Time
Critical P1	An SOC Cybersecurity Analyst will make contact with the customer technical representative within one (1) hour of the request for support being logged in the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action. Continual effort will be maintained to identify the extent of the incident and provide actions for containment.
High P2	An SOC Cybersecurity Analyst will make contact with the customer technical representative within four (4) hours of the request for support being logged at the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action. Continual effort will be maintained to identify the extent of the incident and provide actions for containment.
Medium P3	An SOC Cybersecurity Support Engineer will make contact with the customer technical representative within the next business day of the request for support being logged at the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action.
Low P4	An SOC Cybersecurity Support Engineer will make contact with the Customer technical representative within seven business days of the logged request for support at the issue management system.

3.3.6.2 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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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^{SM} Platform.

3.3.6.3 ActiveEye^{SM} 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^{SM} 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^{SM} Platform which may be impacted by customer configuration changes, telecommunications connectivity, and/or customer network issues/outages.

3.4 Limitations and Exclusion

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.

3.4.1 Service Limitations

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

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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

3.4.3 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).

3.4.4 Third-Party Software and Service Providers, including Resale

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Section 4

Proposal Pricing

4.1 Pricing Summary

Motorola pricing is based on the services and solution presented in Section 2. The addition or deletion of any component(s) may subject the total solution price to modifications. Pricing will remain valid for ninety (90) days.

Description	Price
ASTRO® 25 Managed Detection and Response	$123,459.10
Hardware and Equipment	Included
Installation and Activation Services	Included
Year 1 Subtotal	**$123,459.10**

Initial Subscription Period after Year 1:

Description	Price
Initial Subscription Period - Year 2	$128,397.46
Initial Subscription Period - Year 3	$133,533.36
Initial Subscription Period - Year 4	$138,874.70
Initial Subscription Period - Year 5	$144,429.68

The Total Contract Value for this proposal is: $668,694.31.

4.2 Payment Schedule & Terms

Period of Performance

The initial MDR subscription period of the contract will extend five (5) years from the Commencement Date of Service, defined as the date data is available for analysis, or not later than thirty (30) days after Motorola provides the Customer with necessary hardware or software.

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 full Year 1 amount according to the Pricing table in Section 4.1.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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

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

INFLATION ADJUSTMENT. For multi-year agreements, at the end of the first year of the Agreement and each year thereafter, a CPI percentage change calculation shall be performed using the U.S. Department of Labor, Consumer Price Index, all Items, Unadjusted Urban Areas (CPI-U). Should the annual inflation rate increase greater than 3% during the previous year, Motorola shall have the right to increase all future maintenance prices by the CPI increase amount exceeding 3%. All items, not seasonally adjusted shall be used as the measure of CPI for this price adjustment. Measurement will take place once the annual average for the new year has been posted by the Bureau of Labor Statistics. For purposes of illustration, if in year 5 the CPI reported an increase of 8%, Motorola may increase the Year 6 price by 5% (8%-3% base).

Tax

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

4.3 Invoicing and Shipping Addresses

Invoices will be sent to Customer at the following address:	
Name:	
Address:	
Phone:	
Email:	
Address of Ultimate Destination for Equipment to be Delivered to Customer:	
Name:	
Address:	
Equipment Shipped to Customer at the following address:	
Name:	
Address:	
Phone:	

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Section 5

Contractual Documentation

Motorola Solutions Customer Agreement

This Motorola Solutions Customer Agreement (the "**MCA**") is entered into between Motorola Solutions, Inc., with offices at 500 W. Monroe Street, Suite 4400, Chicago, IL 60661 ("**Motorola**") and the entity set forth in the signature block below ("**Customer**"). Motorola and Customer will each be referred to herein as a "**Party**" and collectively as the "**Parties**". This Agreement (as defined below) is effective as of the date of the last signature (the "**Effective Date**").

1. Agreement.

1.1. Scope; Agreement Documents. This MCA governs Customer's purchase of Products (as defined below) and Services (as defined below) from Motorola. Additional terms and conditions applicable to specific Products and Services are set forth in one or more addenda attached to this MCA (each an "**Addendum**", and collectively the "**Addenda**"). In addition, the Parties may agree upon solution descriptions, equipment lists, statements of work, schedules, technical specifications, and other ordering documents setting forth the Products and Services to be purchased by Customer and provided by Motorola and additional rights and obligations of the Parties (the "**Ordering Documents**", "Initial Order Form", or "Order Form"). To the extent required by applicable procurement law, a proposal submitted by Motorola in response to a competitive procurement process will be included within the meaning of the term Ordering Documents. This MCA, the Addenda, and any Ordering Documents collectively form the Parties' "**Agreement**".

1.2. Order of Precedence. Each Addendum will control with respect to conflicting terms in the MCA, but only as applicable to the Products and Services described in such Addendum. Each Ordering Document will control with respect to conflicting terms in the MCA or any Addenda, but only as applicable to the Products and Services described on such Ordering Document.

2. Products and Services.

2.1. Products. Motorola will provide Cyber Security Detection and Response Solutions through Motorola Solutions Cloud Base Cyber Security Programs, PremierOne Managed Detection & Response and ASTRO 25 Managed Detection and Response, as seen in the attached proposals, dated February 29, 2024, for St. Johns County Communications and Interoperable Radio System Departments.

2.1.1 Non-Preclusion. If, in connection with the Products and Services provided under this Agreement, Motorola makes recommendations, including a recommendation to purchase other products or services, nothing in this Agreement precludes Motorola from participating in a future competitive bidding process or otherwise offering or selling the recommended products or other services to Customer. Customer represents that this paragraph does not violate its procurement standards or other laws, regulations, or policies.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

2.1.2 Customer Obligations. Customer will ensure that information Customer provides to Motorola in connection with receipt of Products and Services are accurate and complete in all material respects. Customer will make timely decisions and obtain any required management approvals that are reasonably necessary for Motorola to provide the Products and Services and perform its other duties under this Agreement. Unless the applicable Ordering Document states otherwise, Motorola may rely upon and is not required to evaluate, confirm, reject, modify, or provide advice concerning any assumptions or Customer information, decisions, or approvals described in this Section. If any assumptions in the Ordering Documents or information provided by Customer prove to be incorrect, or if Customer fails to perform any of its obligations under this Agreement, Motorola's ability to perform its obligations may be impacted and changes to the Agreement, including the scope, Fees, and performance schedule may be required.

2.1.3 Documentation. Products and Services may be delivered with documentation for the Equipment, software Products, or data that specifies technical and performance features, capabilities, users, or operation, including training manuals, and other deliverables, such as reports, specifications, designs, plans, drawings, analytics, or other information (collectively, "**Documentation**"). Documentation is and will be owned by Motorola, unless otherwise expressly agreed in an Addendum or Ordering Document that certain Documentation will be owned by Customer. Motorola hereby grants Customer a limited, royalty-free, worldwide, non-exclusive license to use the Documentation solely for its internal business purposes in connection with the Products and Services.

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

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

2.4 Export Control. Customer, its employees, and any other Authorized Users will not access or use the Products and Services in any jurisdiction in which the provision of such Products and Services is prohibited under applicable laws or regulations (a "**Prohibited Jurisdiction**"), and Customer will not provide access to the Products and Services to any government, entity, or individual located in a Prohibited Jurisdiction. Customer represents and warrants that (a) it and its Authorized Users are not named on any U.S. government list of persons prohibited from receiving U.S. exports, or transacting with any U.S. person; (b) it and its Authorized Users are not a national of, or a company registered in, any Prohibited Jurisdiction; (c) Customer will not permit its Authorized Users to access or use the Products or Services in violation of any U.S. or other applicable export embargoes, prohibitions or

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

restrictions; and (d) Customer and its Authorized Users will comply with all applicable laws regarding the transmission of technical data exported from the U.S. and the country in which Customer, its employees, and the Authorized Users are located.

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

3 Term and Termination.

3.1 Term. The term of this MCA ("**Term**") will commence on the Effective Date and continue until five (5) years, unless the MCA is earlier terminated as set forth herein. The applicable Addendum or Ordering Document will set forth the term for the Products and Services governed thereby.

3.2 Termination. Either Party may terminate the Agreement or the applicable Addendum or Ordering Document if the other Party breaches a material obligation under the Agreement and does not cure such breach within thirty (30) days after receipt of notice of the breach or fails to produce a cure plan within such period of time. Each Addendum and Ordering Document may be separately terminable as set forth therein, however, termination of this Agreement shall constitute termination of all Addendums and Ordering Documents, unless otherwise set forth within the Notice of Termination.

3.2.1 Termination for Non-Appropriation. Customer may terminate this Agreement, with thirty (30) days written notice due to the lack of lawfully appropriated funds in any given Fiscal Year. The termination shall take effect on the last day of the fiscal year for which the appropriation was made without penalty or expense to the Customer.

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

3.4 Effect of Termination or Expiration. Upon termination for any reason or expiration of this Agreement, an Addendum, or an Ordering 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, except that Equipment purchased by Customer should not be returned. If Customer has any outstanding payment obligations under this Agreement, Motorola may accelerate and declare all such obligations of Customer immediately due and payable by Customer. Notwithstanding the reason for termination or expiration, Customer must pay Motorola for Products and Services already delivered. Customer has a duty to mitigate any damages under this Agreement, including in the event of default by Motorola and Customer's termination of this Agreement.

4 Payment and Invoicing.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

4.1 Fees. Customer shall compensate Motorola Solutions in accordance with the mutually agreed to Order Form entered into between the County and Motorola Solutions. The Initial Order Form reflects an Order Total for Year 1 of one hundred twenty three thousand four hundred fiftynine dollars and ten cents, ($123,459.10), which shall be paid according to the ordering document payment schedule.

4.1.1 Customer will make all reasonable efforts to provide funds needed by Motorola Solutions to perform under this Agreement. and as funds are appropriated by their governing board. Customer makes no express commitment to provide such funds in any given Customer Fiscal Year. Moreover, it is expressly noted that Motorola Solutions cannot demand that Customer provide any such funds in any given Customer Fiscal Year.

4.1.2 The Fees for Years 2 through 5, are as provided below, provided the necessary appropriated funds are available for the Services pursuant to this Agreement.

Year	Astro25 Managed Detection
2	$128,397.46
3	$133,533.36
4	$138,874.70
5	$144,429.68

4.1.3 It is strictly understood that Motorola Solutions is not entitled to the above-referenced amount of compensation. Rather, Motorola Solutions compensation shall be based upon Motorola Solutions providing the Services, in accordance with this Agreement.

4.2 Taxes. Motorola Solutions shall pay and be solely responsible for any and all taxes, levies, duties and assessments of every nature which may be applicable to any services performed under this Agreement, including, without limitation, any tax that Motorola Solutions is required to deduct or withhold from any amount payable under this Agreement and shall make all payroll deductions and withholdings required by law. Motorola Solutions herein indemnifies and holds Customer harmless from any liability on account of any and all such taxes, levies, duties, and assessments. The indemnity provision of this Section 4.2 shall survive the expiration or earlier termination of this Agreement. Motorola Solutions shall not use Customer's tax-exempt status unless specifically authorized in writing.

4.2.1 Foreign Entity Tax Withholding. Amounts due to certain foreign persons or entities may be subject to backup withholding taxes under federal law. If Motorola Solutions is a foreign person or entity that is required to complete Internal Revenue Service ("IRS") Form W-8ECI, Motorola Solutions shall provide Customer a copy of current Form W-8ECI prior to issuance of any invoice or payment under this Agreement. If Motorola Solutions fails to timely provide a completed, current Form W-8ECI, Customer will withhold all backup withholding taxes from the amounts due to Motorola Solutions, remit such sums to the IRS, and pay Motorola Solutions only the remainder. Customer makes no representation regarding the tax treatment of amounts due to Motorola Solutions, and Motorola Solutions releases and holds the Customer harmless from any claims or damages in any way relating to or arising from any tax withholding by Customer pursuant to this section.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

4.3 Invoicing. Motorola will invoice Customer for Year 1 upon Contract Execution and Years 2-5 shall be invoiced annually within fifteen (15) days of the anniversary date of the Agreement. Customer will pay all invoices within forty-five (45) days of the invoice date. Late payments will be subject to interest charges at the maximum rate permitted by law, commencing upon the due date. Motorola may invoice electronically via email, and Customer agrees to receive invoices via email at the email address set forth in an Ordering Document. Customer acknowledges and agrees that a purchase order or other notice to proceed is not required for payment for Products or Services.

5 Sites; Customer-Provided Equipment; Non-Motorola Content.

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

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

5.3 Site Issues. Motorola will have the right at any time to inspect the Sites and advise Customer of any deficiencies or non-conformities with the requirements of this **Section 5 – Sites; Customer-Provided Equipment; Non-Motorola Content**. If Motorola or Customer identifies any deficiencies or non-conformities, Customer will promptly remediate such issues or the Parties will select a replacement Site. If a Party determines that a Site identified in an Ordering Document is not acceptable or desired, the Parties will cooperate to investigate the conditions and select a replacement Site or otherwise adjust the installation plans and specifications as necessary. A change in Site or adjustment to the installation plans and specifications may cause a change in the Fees or performance schedule under the applicable Ordering Document.

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

5.5 Non-Motorola Content. In certain instances, Customer may be permitted to access, use, or integrate Customer or third-party software, services, hardware, content, and data that is not provided by Motorola (collectively, "**Non-Motorola Content**") with or through the Products and Services. If Customer accesses, uses, or integrates any Non-Motorola Content with the Products or 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 Products and Services. Customer will also obtain the necessary rights for Motorola to use such Non-Motorola Content in connection with providing the Products and Services, including the right for Motorola to access, store, and process such Non-Motorola Content (e.g., in connection with Subscription Software), and to otherwise enable interoperation with the Products and 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 Products and 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 Products and 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 Products and Services). If Customer receives notice that any Non-Motorola Content must be removed, modified, or disabled within the Products or 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 Products or Services, Motorola, Motorola's systems, or any third party (including other Motorola customers). Motorola may provide certain Non-Motorola Content as an authorized sales representative of a third party as set out in an Ordering Document. As an authorized sales representative, the third party's terms and conditions, as set forth in the Ordering Document, will apply to any such sales. Any orders for such Non-Motorola Content will be filled by the third party. Nothing in this Section will limit the exclusions set forth in **Section 7.2 – Intellectual Property Infringement**.

5.6 End User Licenses. Notwithstanding any provision to the contrary in the Agreement, certain Non-Motorola Content software are governed by a separate license, EULA, or other agreement, including terms governing third-party equipment or software, such as open source software, included in the Products and Services. Customer will comply, and ensure its Authorized Users comply, with any such additional terms applicable to third-party equipment or software. If provided for in the separate third party license, Customer may have a right to receive source code for such software; a copy of such source code may be obtained free of charge by contacting Motorola.

6 Representations and Warranties.

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Addendum or Ordering Document. Motorola provides other express warranties for Motorola-manufactured Equipment, Motorola-owned software Products, and certain Services. Such express warranties are included in the applicable Addendum or Ordering Document. Such representations and warranties will apply only to the applicable Product or Service that is the subject of such Addendum or Ordering Document.

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

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

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

7 Indemnification.

7.3 General Indemnity. Motorola will defend, indemnify, and hold harmless Customer, its officers, and employees from and against any and all damages, losses, liabilities, and expenses, including but not limited to reasonable attorneys' fees, arising from any third party actual claim, demand, action, or proceeding ("**Claim**") for personal injury, death, or direct damage to tangible property to the extent caused by Motorola's gross negligence, recklessness, or intentionally wrongful conduct of Motorola Solutions or other persons employed or utilized by Motorola Solutions in the performance of services under this Agreement; except to the extent the Claim arises from Customer's negligence or willful misconduct. Motorola's duties under this **Section 7.1 – General Indemnity** are conditioned upon: (a) Customer promptly notifying Motorola in writing of the Claim; (b) Motorola having sole control of the defense of the suit and all negotiations for its settlement or compromise; and (c) Customer cooperating with Motorola and, if requested by Motorola, providing reasonable assistance in the defense of the Claim.

7.3.1 To the extent permitted by applicable law, Motorola Solutions further agrees that "damages, losses, and costs", includes fines, citations, court judgments, insurance claims, restoration costs, or other liability, to the extent caused by the gross negligence, recklessness, or intentionally wrongful conduct of Motorola Solutions and person employed or utilized by Motorola Solutions in the performance of Services under this Agreement.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

7.3.2 To the extent permitted by applicable law, for purposes of indemnity, the "persons employed or utilized by Motorola Solutions" shall be construed to include, but not be limited to, Motorola Solutions, its staff, employees, subcontractors, all deliverers, suppliers, furnishers of materials or services or anyone acting for, on behalf of, or at the request of Motorola Solutions.

7.4 Intellectual Property Infringement. Motorola will defend Customer against any third-party claim alleging that a Motorola-developed or manufactured Product or Service (the "**Infringing Product**") directly infringes a United States patent or copyright ("**Infringement Claim**"), and Motorola will pay all damages finally awarded against Customer by a court of competent jurisdiction for an Infringement Claim, or agreed to in writing by Motorola in settlement of an Infringement Claim. Motorola's duties under this **Section 7.2 – Intellectual Property Infringement** are conditioned upon: (a) Customer promptly notifying Motorola in writing of the Infringement Claim; (b) Motorola having sole control of the defense of the suit and all negotiations for its settlement or compromise; and (c) Customer cooperating with Motorola and, if requested by Motorola, providing reasonable assistance in the defense of the Infringement Claim.

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

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

7.4.3 This **Section 7.2 – Intellectual Property Infringement** provides Customer's sole and exclusive remedies and Motorola's entire liability in the event of an Infringement Claim. For clarity, the rights and remedies provided in this Section are subject to, and limited by, the restrictions set forth in **Section 8 – Limitation of Liability** below.

7.5 Customer Indemnity. Customer will defend, indemnify, and hold Motorola and its subcontractors, subsidiaries and other affiliates harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual or threatened third-party claim, demand, action, or proceeding arising from or related to (a) Customer-Provided Equipment, Customer Data, or Non-Motorola Content, including any claim, demand, action, or proceeding alleging that any such equipment, data, or materials (or the integration or use thereof with the Products and Services) infringes or misappropriates a third-party intellectual property or other right, violates applicable law, or breaches the Agreement; (b) Customer-Provided

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Equipment's failure to meet the minimum requirements set forth in the applicable Documentation or match the applicable specifications provided to Motorola by Customer in connection with the Products or Services; (c) Customer's (or its service providers, agents, employees, or Authorized User's) negligence or willful misconduct; and (d) Customer's or its Authorized User's breach of this Agreement. This indemnity will not apply to the extent any such claim is caused by Motorola's use of Customer-Provided Equipment, Customer Data, or Non-Motorola Content in violation of the Agreement. Motorola will give Customer prompt, written notice of any claim subject to the foregoing indemnity. Motorola will, at its own expense, cooperate with Customer in its defense or settlement of the claim.

8 Limitation of Liability.

8.1 DISCLAIMER OF CONSEQUENTIAL DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, MOTOROLA, ITS AFFILIATES, AND ITS AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, SUBCONTRACTORS, AGENTS, SUCCESSORS, AND ASSIGNS (COLLECTIVELY, THE "**MOTOROLA PARTIES**") WILL NOT BE LIABLE IN CONNECTION WITH THIS AGREEMENT (WHETHER UNDER MOTOROLA'S INDEMNITY OBLIGATIONS, A CAUSE OF ACTION FOR BREACH OF CONTRACT, UNDER TORT THEORY, OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOST PROFITS OR REVENUES, EVEN IF MOTOROLA HAS BEEN ADVISED BY CUSTOMER OR ANY THIRD PARTY OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES AND WHETHER OR NOT SUCH DAMAGES OR LOSSES ARE FORESEEABLE.

8.2 DIRECT DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, THE TOTAL AGGREGATE LIABILITY OF THE MOTOROLA PARTIES, WHETHER BASED ON A CLAIM IN CONTRACT OR IN TORT, LAW OR EQUITY, RELATING TO OR ARISING OUT OF THE AGREEMENT WILL NOT EXCEED THE FEES SET FORTH IN THE ORDERING DOCUMENT UNDER WHICH THE CLAIM AROSE. NOTWITHSTANDING THE FOREGOING, FOR ANY SUBSCRIPTION SOFTWARE OR FOR ANY RECURRING SERVICES, THE MOTOROLA PARTIES' TOTAL LIABILITY FOR ALL CLAIMS RELATED TO SUCH PRODUCT OR RECURRING SERVICES IN THE AGGREGATE WILL NOT EXCEED THE TOTAL FEES PAID FOR SUCH SUBSCRIPTION SOFTWARE OR RECURRING SERVICE, AS APPLICABLE, DURING THE CONSECUTIVE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT FROM WHICH THE FIRST CLAIM AROSE.

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

8.4 Voluntary Remedies. Motorola is not obligated to remedy, repair, replace, or refund the purchase price for the disclaimed issues in **Section 8.3 – Additional Exclusions** above, but if Motorola agrees to provide Services to help resolve such issues, Customer will reimburse Motorola for its reasonable time and expenses, including by paying Motorola any Fees set forth in an Ordering Document for such Services, if applicable.

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

9 Confidentiality.

9.3 Confidential Information. "**Confidential Information**" means any and all non-public information provided by one Party ("**Discloser**") to the other ("**Recipient**") that is disclosed under this Agreement in oral, written, graphic, machine recognizable, or sample form, being clearly designated, labeled or marked as confidential or its equivalent or that a reasonable businessperson would consider non-public and confidential by its nature. With respect to Motorola, Confidential Information will also include Products and Services, and Documentation, as well as any other information relating to the Products and Services. The nature and existence of this Agreement are considered Confidential Information of the Parties. In order to be considered Confidential Information, information that is disclosed orally must be identified as confidential at the time of disclosure and confirmed by Discloser by submitting a written document to Recipient within thirty (30) days after such disclosure. The written document must contain a summary of the Confidential Information disclosed with enough specificity for identification purpose and must be labeled or marked as confidential or its equivalent.

9.4 Obligations of Confidentiality. During the Term and for a period of three (3) years from the expiration or termination of this Agreement, Recipient will (a) not disclose Confidential Information to any third party, except as expressly permitted in this **Section 9 - Confidentiality**; (b) restrict disclosure of Confidential Information to only those employees (including, employees of any wholly owned subsidiary, a parent company, any other wholly owned subsidiaries of the same parent company), agents or consultants who must access the Confidential Information for the purpose of, and who are bound by confidentiality terms substantially similar to those in, this Agreement; (c) not copy, reproduce, reverse engineer, de-compile or disassemble any Confidential Information; (d) use the same degree of care as for its own information of like importance, but at least use reasonable care, in safeguarding against disclosure of Confidential Information; (e) promptly notify Discloser upon discovery of any unauthorized use or disclosure of the Confidential Information and take reasonable steps to regain possession of the Confidential Information and prevent further unauthorized actions or other breach of this Agreement; and (f) only use the Confidential Information as needed to fulfill its obligations and secure its rights under this Agreement.

9.5 Exceptions. Recipient is not obligated to maintain as confidential any information that Recipient can demonstrate by documentation (a) is publicly available at the time of disclosure or becomes available to the public without breach of this Agreement; (b) is lawfully obtained from a third party without a duty of confidentiality to Discloser; (c) is otherwise lawfully known to Recipient prior to such disclosure without a duty of confidentiality to Discloser; or (d) is independently developed by Recipient without the use of, or reference to, any of Discloser's Confidential Information or any breach of this Agreement. Additionally, Recipient may disclose Confidential Information to the extent required by law, including a judicial or legislative order or proceeding.

9.6 Ownership of Confidential Information. All Confidential Information is and will remain the property of Discloser and will not be copied or reproduced without the express written permission of

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Discloser (including as permitted herein). Within ten (10) days of receipt of Discloser's written request, Recipient will return or destroy all Confidential Information to Discloser along with all copies and portions thereof, or certify in writing that all such Confidential Information has been destroyed. However, Recipient may retain (a) one (1) archival copy of the Confidential Information for use only in case of a dispute concerning this Agreement and (b) Confidential Information that has been automatically stored in accordance with Recipient's standard backup or recordkeeping procedures, provided, however that Recipient will remain subject to the obligations of this Agreement with respect to any Confidential Information retained subject to clauses (a) or (b). No license, express or implied, in the Confidential Information is granted to the Recipient other than to use the Confidential Information in the manner and to the extent authorized by this Agreement. Discloser represents and warrants that it is authorized to disclose any Confidential Information it discloses pursuant to this Agreement.

10 Proprietary Rights; Data; Feedback.

10.3 Data Definitions. The following terms will have the stated meanings: "**Customer Contact Data**" means data Motorola collects from Customer, its Authorized Users, and their end users for business contact purposes, including marketing, advertising, licensing and sales purposes; "**Service Use Data**" means data generated by Customer's use of the Products and Services or by Motorola's support of the Products and Services, including personal information, product performance and error information, activity logs and date and time of use; "**Customer Data**" means data, information, and content, including images, text, videos, documents, audio, telemetry, location 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 Products and Services. Customer Data does not include Customer Contact Data, Service Use Data, or information from publicly available sources or other Third-Party Data or Motorola Data; **"Third-Party Data"** means information obtained by Motorola from publicly available sources or its third party content providers and made available to Customer through the Products or Services; "**Motorola Data**" means data owned or licensed by Motorola; "**Feedback**" means 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 Products or Services; and **"Process"** or **"Processing"** means any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, copying, analyzing, caching, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

10.4 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 Products and Services, Motorola 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 Addendum or Ordering Document, 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 Agreement does not grant to Customer any shared development rights in or to any Motorola Materials or other intellectual property, and Customer agrees to execute any documents and take any other actions reasonably requested by Motorola to effectuate the foregoing. Motorola and its licensors reserve all rights not expressly granted to Customer, and no rights, other than those expressly granted herein, are granted to Customer by

implication, estoppel or otherwise. Customer will not modify, disassemble, reverse engineer, derive source code or create derivative works from, merge with other software, distribute, sublicense, sell, or export the Products and Services or other Motorola Materials, or permit any third party to do so.

10.5 Ownership of Customer Data. Customer retains all right, title and interest, including intellectual property rights, if any, in and to Customer Data. Motorola acquires no rights to Customer Data except those rights granted under this Agreement including the right to Process and use the Customer Data as set forth in **Section 10.4 – 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 10.4.3 – Sub-processors**.

10.6 Processing Customer Data.

10.6.1 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) to (a) perform Services and provide Products under the Agreement, (b) analyze the Customer Data to operate, maintain, manage, and improve Motorola Products and Services, and (c) create new products and services. Customer agrees that this Agreement, 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.

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

10.6.3 Sub-processors. Customer agrees that Motorola may engage sub-processors who in turn may engage additional sub-processors to Process personal data in accordance with this Agreement. When engaging sub-processors, Motorola will enter into agreements with the sub-processors to bind them to data processing obligations to the extent required by law.

10.7 Data Retention and Deletion. Except as expressly provided otherwise under the Agreement, Motorola will delete all Customer Data following termination or expiration of this MCA or the applicable Addendum or Ordering 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 13.9 – Notices**. 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 Ordering Document.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

10.8 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. Service Use Data may be disclosed to third parties. 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.

10.9 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 Motorola Data and Third-Party Data as permitted by Motorola and the applicable Third-Party Data provider, as described in the applicable Addendum. Unless expressly permitted in the 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 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 Motorola Data or Third-Party Data will immediately terminate upon termination or expiration of the applicable Addendum, Ordering Document, or this MCA. 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 Motorola's agreement with the applicable Third-Party Data provider. Upon termination of Customer's rights to use 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 will have no liability for Third-Party Data or Motorola Data available through the Products and Services. Motorola and its Third-Party Data providers reserve all rights in and to Motorola Data and Third-Party Data not expressly granted in an Addendum or Ordering Document.

10.10 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.

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

11 Force Majeure; Delays Caused by Customer.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

11.3 Force Majeure. Neither Party will be responsible for nonperformance or delayed performance due to events that are not reasonably foreseeable and are outside of its reasonable control. If performance will be significantly delayed, the affected Party will provide notice to the other Party, and the Parties will agree (in writing) upon a reasonable extension to any applicable performance schedule.

11.4 Delays Caused by Customer. Motorola's performance of the Products and Services will be excused for delays caused by Customer or its Authorized Users or subcontractors, or by failure of any assumptions set forth in this Agreement (including in any Addendum or Ordering Document). In the event of a delay under this **Section 11.2 – Delays Caused by Customer**, (a) Customer will continue to pay the Fees as required hereunder, (b) the Parties will agree (in writing) upon a reasonable extension to any applicable performance schedule, and (c) Customer will compensate Motorola for its out-of-pocket costs incurred due to the delay (including those incurred by Motorola's affiliates, vendors, and subcontractors).

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

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

12.4 Negotiation. Either Party may initiate dispute resolution procedures by sending a notice of Dispute ("**Notice of Dispute**") to the other Party. The Parties will attempt to resolve the Dispute promptly through good faith negotiations, including timely escalation of the Dispute to executives who have authority to settle the Dispute (and who are at a higher level of management than the persons with direct responsibility for the matter). All communication relating to the Dispute resolution will be maintained in strict confidence by the Parties. Notwithstanding the foregoing, any Dispute arising from or relating to Motorola's intellectual property rights will not be subject to negotiation in accordance with this Section, but instead will be decided by a court of competent jurisdiction, in accordance with **Section 12.3 – Litigation, Venue, Jurisdiction** below.

12.5 Litigation, Venue, Jurisdiction. If the Dispute has not been resolved within sixty (60) days from the Notice of Dispute, either Party may submit the Dispute exclusively to a court in St. Johns County, FL. Each Party expressly consents to the exclusive jurisdiction of such courts for resolution of any Dispute.

13 General.

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

13.4 Audit; Monitoring. Motorola will have the right to monitor and audit use of the Products, which may also include access by Motorola to Customer Data and Service Use Data. Customer will provide notice of such monitoring to its Authorized Users and obtain any required consents, including individual end users, and will cooperate with Motorola in any monitoring or audit. Customer will maintain during the Term, and for two (2) years thereafter, accurate records relating to any software licenses granted under this Agreement to verify compliance with this Agreement. Motorola or a third party ("**Auditor**") may inspect Customer's and, as applicable, Authorized Users' premises, books, and records. Motorola will pay expenses and costs of the Auditor, unless Customer is found to be in violation of the terms of the Agreement, in which case Customer will be responsible for such expenses and costs.

13.5 Assignment and Subcontracting. Neither Party may assign or otherwise transfer this Agreement without the prior written consent of the other Party, which will not be unreasonably withheld. Subject to the foregoing, this Agreement will be binding upon the Parties and their respective successors and assigns.

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

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

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

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

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

13.11 Notices. Any and all notices, requests, consents approvals, demands, determinations, instructions, and other forms of written communication ("Notices") under this Agreement shall be validly given when delivered as follows:

1. Hand delivered to Consultant's Authorized Representative or hand delivered during normal business hours and addressed as shown below; or

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

2. Delivered by U.S. Mail, electronic mail or commercial express carrier, (postage prepaid, delivery receipt requested), to the following addresses:

St. Johns County 500 San Sebastian View St. Augustine, FL 32084 Attn: Leigh Daniels Email Address: ldaniels@sjcfl.us	Motorola Solutions 500 West Monroe Street Chicago, IL 60661 Attn: Rodrigo Olzazbal Email Address: rodrigo.olazabal1@motorolasolutions.com

With a copy to:
St. Johns County
Office of the County Attorney 500 San Sebastian View
St. Augustine, FL 32084
Email Address: BCCAttorney@sjcfl.us

3. Notices shall be deemed to have been given on the date of delivery to the location listed above without regard to actual receipt by the named addressee. County and Motorola Solutions may each change the above address at any time upon prior written notice to the other party.

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

13.13 Insurance Requirements. Motorola Solutions shall not commence work under this Contract until it has obtained all insurance required under this section. All insurance policies shall be issued by companies authorized to do business under the laws of the State of Florida. Motorola Solutions shall furnish proof of Insurance to the County prior to the commencement of operations. The Certificate(s) shall clearly indicate Motorola Solutions has obtained insurance of the type, amount, and classification as required by contract and that it will provide written notice within thirty (30) days of cancellation of the insurance. Compliance with the foregoing requirements shall not relieve Motorola Solutions of its liability and obligations under this Contract.

Certificate Holder Address:	St. Johns County, a political subdivision of the State of Florida 500 San Sebastian View St. Augustine, FL 32084

13.13.1 Motorola Solutions shall maintain during the life of this Agreement, Comprehensive General Liability Insurance with limits of $1,000,000 per occurrence, $2,000,000 aggregate to protect Motorola Solutions from claims for damages for bodily injury, including wrongful death, as well as from claims of property damages which may arise from any operations under this Agreement, whether such operations be by Motorola Solutions or by anyone directly employed by or contracting with Motorola Solutions.

13.13.2 Motorola Solutions shall maintain during the life of this Contract, Technology Errors & Omissions/Professional Liability with limits of $3,000,000 per claim and aggregate. The Technology Errors & Omissions/Professional Liability Insurance shall cover Motorola Solutions and third parties, at a minimum, the following: Liability for Technology Products/Services, Data Breach, Media Content,

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Privacy Liability, and Network Security. Coverage retro date shall be prior to commencement of job.

13.13.3 Motorola Solutions shall maintain during the life of this Contract Errors and Omissions / Cyber Liability & Data Storage Insurance with limits of $3,000,000 per claim, $3,000,000 aggregate. The Cyber Liability Insurance shall cover, at a minimum, the following: Data Loss and System Damage Liability; Security Liability; Privacy Liability; and Privacy/Security Breach Response Coverage, including Notification Expenses. The Cyber Liability Insurance may be included as part of the Professional Liability Insurance required above.

13.13.4 Motorola Solutions shall maintain during the life of this Contract, adequate Workers' Compensation Insurance in at least such amounts as is required by the law for all of its employees per Florida Statute 440.02.

13.14 Public Records.

A) The cost of reproduction, access to, disclosure, non-disclosure, or exemption of records, data, documents, and/or materials, associated with this Agreement shall be subject to the applicable provisions of the Florida Public Records Law (Chapter 119, Florida Statutes), and other applicable State and Federal provisions. Access to such public records, may not be blocked, thwarted, and/or hindered by placing the public records in the possession of a third party, or an unaffiliated party.

B) In accordance with Florida law, to the extent that Motorola Solutions performance under this Agreement constitutes an act on behalf of the County, Motorola Solutions shall comply with all requirements of Florida's public records law. Specifically, if Motorola Solutions is expressly authorized, and acts on behalf of the County under this Agreement, Motorola Solutions shall:

1) Keep and maintain public records that ordinarily and necessarily would be required by the County in order to perform the services described herein;

2) Upon request from the County's custodian of public records, provide the County with a copy of the requested records or allow the records to be inspected or copied with a reasonable time at a cost that does not exceed the cost as provided in Chapter 119, Florida States, or as otherwise provided by applicable law;

3) Ensure that public records related to this Agreement that are exempt or confidential and exempt from public disclosure requirements are not disclosed except as authorized by applicable law for the duration of this Agreement and the following completion of this Agreement if Motorola Solutions does not transfer the records to the County; and

4) Meet all requirements for retaining public records, and transfer at Motorola Solutions sole cost and expense, all public records in the possession of Motorola Solutions upon termination of this Agreement. Motorola Solutions shall destroy any duplicate records that are exempt or confidential and exempt from public disclosure requirements in accordance with applicable State and Federal provisions. Any public records stored electronically must be provided to the County in a format that is compatible with information technology systems maintained by the County.

C) If Motorola Solutions transfers all public records to the County upon completion of this Agreement, Motorola Solutions shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If Motorola Solutions

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

keeps and maintains public records upon completion of this Agreement, Motorola Solutions shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the County, upon request from the County's custodian of public records, in a format that is compatible with the County's information technology systems.

D) Failure by the Motorola Solutions to comply with the requirements of this section shall be grounds for immediate, unilateral termination of this Agreement by the County.

IF MOTOROLA SOLUTIONS HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO ITS DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT: 500 San Sebastian View St. Augustine, FL 32084 (904) 209-0805; publicrecords@sjcfl.us.

E) Failure by Motorola Solutions to grant such public access shall be grounds for immediate, unilateral termination of this Agreement by the County. Motorola Solutions shall promptly provide the County notice of any request to inspect or copy public records related to this Agreement in Motorola Solutions possession and shall promptly provide the County a copy of Motorola Solutions response to each such request.

13.15 Survival. The following provisions will survive the expiration or termination of this Agreement for any reason: **Section 2.4 – Customer Obligations**; **Section 3.4 – Effect of Termination or Expiration**; **Section 4 – Payment and Invoicing**; **Section 6.5 – Warranty Disclaimer**; **Section 7.3 – Customer Indemnity**; **Section 8 – Limitation of Liability**; **Section 9 – Confidentiality**; **Section 10 – Proprietary Rights; Data**; **Feedback**; **Section 11 – Force Majeure; Delays Caused by Customer**; **Section 12 – Disputes**; and **Section 13 – General**.

13.16 Amendments & Modifications. This Agreement shall not be modified, amended, changed or supplemented, nor may any obligations hereunder be waived or extensions of time for performance granted, except by written instrument signed by authorized representatives of both Parties. No waiver of any default or breach of any obligation or provision herein contained shall be deemed a waiver of any preceding or succeeding default or breach thereof or of any other agreement or provision herein contained. No extension of time for performance of any obligations or acts shall be deemed an extension of time for performance of any other obligations or acts.

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

amendment or modification or part of this Agreement, even if a representative of each Party signs such document.

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

Motorola: Motorola Solutions, Inc.	**Customer:** _____
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Cyber Addendum

Motorola Solutions Inc. ("**Motorola**") and the customer named in the Agreement to which this Cyber Addendum (the "**Addendum**") is attached ("**Customer**") hereby agree as follows:

Section 6Section 1. APPLICABILITY

1.1 This Addendum sets out terms applicable to Customer's purchase of cyber security services that are in addition to, and that may in some respects amend or supersede, terms in the Agreement

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

pertaining to (i) Remote Security Update Service, Security Update Service, and Managed Detection & Response subscription services, among other subscription services ("**Subscription Services**"),(ii) professional services ("**Professional Services**"), and/or (iii) retainer services (i.e., professional services when expressly purchased as a block of pre-paid hours for use, subject to expiration, within a specified period across certain offered service categories ("**Retainer Services**") (all collectively herein, "**Services**").

Section 7Section 2. ADDITIONAL DEFINITIONS AND INTERPRETATION

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

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

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

2.4 "**Feedback**" means 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 Services. Any Feedback provided by Customer is entirely voluntary. Motorola may use, reproduce, license, and otherwise distribute and exploit the Feedback without any obligation or payment to Customer or Authorized Users. Customer represents and warrants that it has obtained all necessary rights and consents to grant Motorola the foregoing rights.

2.5 "**Motorola Data**" has the meaning given to it in the DPA.

2.6 "**Process**" or "**Processing**" has the meaning given to it in the DPA.

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

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

2.9 "**Third-Party Data**" has the meaning given to it in the DPA.

Section 8Section 3. LICENSE, DATA AND SERVICE CONDITIONS

3.1 Delivery of Cyber Services

3.1.1 All Professional Services will be performed in accordance with the performance

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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

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

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

3.2 Motorola may use or provide Customer with access to software, tools, enhancements, updates, data, derivative works, and other materials which Motorola has developed or licensed from third parties (collectively, "**Motorola Materials**"). The Services, Motorola Data, Third-Party Data, and related documentation, are considered Motorola Materials. Notwithstanding the use of such materials in Services or Deliverables, 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 Deliverables and the Motorola Materials. Motorola grants Customer and Authorized Users a limited, non-transferable, non-sublicensable, and non-exclusive license to use the Services and associated Deliverables solely for Customer's internal business purposes.

3.2.1 Motorola may use, engage, resell, or otherwise interface with third-party software, hardware or services providers (such as, for example, third-party end point detection and response providers) and other sub-processors, who in turn may engage additional sub-processors to process personal data and other Customer Data. Customer agrees that such third-party software or services providers, sub-processors or their respective sub-processors may process and use personal and other Customer Data in accordance with and subject to their own respective licenses or terms and in accordance with applicable law. Customer authorizes and will provide and obtain all required notices and consents, if any, and comply with other applicable legal requirements, if any, with respect to such collection and use of personal data and other Customer Data by Motorola, and its subcontractors, sub-processors and/or third-party software, hardware or services providers.

3.2.2 In addition to terms set forth in this Addendum, certain components of the Subscription Services and the Motorola Materials may be governed by one or more third-party End User License Agreements ("**EULA**"), which include terms governing third-party software licensed to Motorola ("**Licensed Software**"), such as open source software, included in the Subscription Services and/or the Motorola Materials. Customer will comply, and ensure its Authorized Users comply, with such additional license agreements. EULAs for the Licensed Software are linked through the proposal to which this Addendum is attached.

3.3 To the extent Customer is permitted to access, use, or integrate Customer or third-party software, services, content, or data that is not provided by Motorola (collectively, "**Non-Motorola**

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Content") with or through the Services, or will use equipment or software not provided by Motorola, which may be required for use of the Services ("**Customer-Provided Equipment**"), Customer will obtain and continuously maintain all rights and licenses necessary for Motorola to efficiently perform all contemplated Services under this Addendum and will assume responsibility for operation and integration of such content and equipment.

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

3.5 Motorola Use of Customer Data. Notwithstanding any provision to the contrary in this Addendum or any related agreement, and except as may be provided to the contrary in the DPA, and in addition to other uses and rights set out herein, 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.

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

3.7 Beta or Proof of Concept Services. If Motorola makes any beta version of its Services ("**Beta Service**") available to Customer, or provides Customer a trial period or proof of concept period (or other demonstration) of the Services at reduced or no charge ("**Proof of Concept**" or "**POC Service**"), Customer may choose to use such Beta or POC Service at its own discretion, provided, however, that Customer will use the Beta or POC Service solely for purposes of Customer's evaluation of such Beta or POC Service, and for no other purpose. Customer acknowledges and agrees that all Beta or POC Services are offered "as-is" and without any representations or warranties or other commitments or protections from Motorola. Motorola will determine the duration of the evaluation period for any Beta or POC Service, in its sole discretion, and Motorola may discontinue any Beta or POC Service at any time. Customer acknowledges that Beta Services, by their nature, have not been fully tested and may contain defects or deficiencies. Notwithstanding any other provision of this Agreement, to the extent a future paid Service has been agreed upon subject to and contingent on the Customer's evaluation of a Proof of Concept Service, Customer may cancel such future paid Service as specified in the SOW or, if not specified, within a reasonable time before the paid Service is initiated.

Section 9Section 4. WARRANTY

4.1 CUSTOMER ACKNOWLEDGES, UNDERSTANDS AND AGREES THAT MOTOROLA DOES NOT GUARANTEE OR WARRANT THAT IT WILL DISCOVER ALL OF CUSTOMER'S

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

SECURITY EVENTS (SUCH EVENTS INCLUDING THE UNAUTHORIZED ACCESS, ACQUISITION, USE, DISCLOSURE, MODIFICATION OR DESTRUCTION OF CUSTOMER DATA), THREATS, OR SYSTEM VULNERABILITIES. MOTOROLA DISCLAIMS ANY AND ALL RESPONSIBILITY FOR ANY AND ALL LOSS OR COSTS OF ANY KIND ASSOCIATED WITH SECURITY EVENTS, THREATS OR VULNERABILITIES WHETHER OR NOT DISCOVERED BY MOTOROLA. MOTOROLA DISCLAIMS ANY RESPONSIBILITY FOR CUSTOMER'S USE OR IMPLEMENTATION OF ANY RECOMMENDATIONS PROVIDED IN CONNECTION WITH THE SERVICES. IMPLEMENTATION OF RECOMMENDATIONS DOES NOT ENSURE OR GUARANTEE THE SECURITY OF THE SYSTEMS AND OPERATIONS EVALUATED. CUSTOMER SHALL BE RESPONSIBLE TO TAKE SUCH ACTIONS NECESSARY TO MITIGATE RISKS TO ITS OPERATIONS AND PROTECT AND PRESERVE ITS COMPUTER SYSTEMS AND DATA, INCLUDING CREATION OF OPERATIONAL WORKAROUNDS, BACKUPS AND REDUNDANCIES.

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

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

4.4 Motorola warrants that the Services will be performed in a professional and workmanlike manner and will conform in all material respects to the SOW(s). This warranty will be for a period of ninety (90) days following completion of the Services. If Motorola breaches this warranty, Customer's sole and exclusive remedy is to require Motorola to re-perform the non-conforming Services or to refund, on a pro- rata basis, the fees paid for the non- conforming Services. OTHER THAN THOSE WARRANTIES SET FORTH IN THIS SECTION 4, MOTOROLA DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED. Customer acknowledges that the Deliverables for the Subscription Services may contain recommendations, suggestions or advice from Motorola to Customer (collectively, "recommendations"). Motorola makes no warranties concerning those recommendations, and Customer alone accepts responsibility for choosing whether and how to implement the recommendations and the results to be realized from implementing them.

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Section 10Section 5 LIMITATION OF LIABILITY

5.1. DISCLAIMER OF CONSEQUENTIAL DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, MOTOROLA, ITS AFFILIATES, AND ITS AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, SUBCONTRACTORS, AGENTS, SUCCESSORS, AND ASSIGNS (COLLECTIVELY, THE "**MOTOROLA PARTIES**") WILL NOT BE LIABLE IN CONNECTION WITH SERVICES PROVIDED UNDER THIS ADDENDUM (WHETHER UNDER MOTOROLA'S INDEMNITY OBLIGATIONS, A CAUSE OF ACTION FOR BREACH OF CONTRACT, UNDER TORT THEORY, OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOST PROFITS OR REVENUES, EVEN IF MOTOROLA HAS BEEN ADVISED BY CUSTOMER OR ANY THIRD PARTY OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES AND WHETHER OR NOT SUCH DAMAGES OR LOSSES ARE FORESEEABLE.

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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

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

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Data Processing Addendum

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

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

1. Definitions.

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

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

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

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

"Data Subjects" means the identified or identifiable person to whom Personal Data relates.

"Metadata" means data that describes other data.

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

"Personal Data" or **"Personal Information"** means any information relating to an identified or identifiable natural person transmitted to Motorola by, through, or on behalf of Customer and its Authorized Users or their end users as part of Customer Data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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

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

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

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

2. Processing of Customer Data

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

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

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

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

a duty of confidentiality, with respect to the handling of Customer Data and any Personal Data contained in Service Use Data.

2.5. Customer's Obligations. Customer is solely responsible for its compliance with all Data Protection Laws and establishing and maintaining its own policies and procedures to ensure such compliance. Customer must not use the Products and Services in a manner that would violate applicable Data Protection Laws. Customer must have sole responsibility for (i) the lawfulness of any transfer of Personal Data to Motorola, (ii) the accuracy, quality, and legality of Personal Data provided to Motorola; (iii) the means by which Customer acquired Personal Data, and (iv) the provision of any required notices to, and obtaining any necessary acknowledgements, authorizations or consents from Data Subjects. Customer takes full responsibility to keep the amount of Personal Data provided to Motorola to the minimum necessary for Motorola to perform in accordance with the Agreement. Customer must be solely responsible for its compliance with applicable Data Protection Laws. Customer agrees that it has implemented administrative, physical and technical safeguards for Customer's environment and operations that are no less rigorous than accepted industry practices and shall ensure that all such safeguards comply with applicable data protection and privacy laws. Customer agrees that Motorola shall not be liable for any Security Incident arising from Customer's breach of this requirement.

2.6. Customer Indemnity. Customer will defend, indemnify, and hold Motorola and its subcontractors, subsidiaries and other affiliates harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual or threatened third-party claim, demand, action, or proceeding arising from or related to Customer's failure to comply with its obligations under this Agreement and/or applicable Data Protection Laws. Motorola will give Customer prompt, written notice of any claim subject to the foregoing indemnity. Motorola will, at its own expense, cooperate with Customer in its defense or settlement of the claim.

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

4. Third-Party Data and Motorola Data. Motorola Data and Third Party Data may be available to Customer through the Products and Services. Customer and its Authorized Users may use the Motorola Data and Third Party Data as permitted by Motorola and the applicable third-party data provider, as described in the Agreement or applicable Addendum. Unless expressly permitted in the Agreement or applicable Addendum, Customer must not, and must ensure its Authorized Users must not: (a) use the Motorola Data or Third-Party Data for any purpose other than Customer's internal business purposes or disclose the data to third parties; (b) "white label" such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (c) use such data in violation of applicable laws ; (d) use such data for activities or purposes where reliance upon the data could lead to death, injury, or property damage; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data; or (f) modify such data or combine it with Customer Data or other data or use the data to build databases. Additional restrictions may be set forth in the Agreement or applicable Addendum. Any rights granted to Customer or Authorized Users with respect to Motorola Data or Third-Party Data must immediately terminate upon termination or expiration of the applicable Addendum, Ordering Document, or the MCA. 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-

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Party Data if Motorola or such Third Party Data provider believes Customer's or the Authorized User's use of the data violates the Agreement, applicable law or by Motorola's agreement with the applicable Third Party Data provider. Upon termination of Customer's rights to use of any Motorola Data or Third-Party Data, Customer and all Authorized Users must immediately discontinue use of such data, delete all copies of such data, and certify such deletion to Motorola. Notwithstanding any provision of the Agreement to the contrary, Motorola has no liability for Third-Party Data or Motorola Data available through the Products and Services. Motorola and its Third Party Data providers reserve all rights in and to Motorola Data and Third-Party Data not expressly granted in an Addendum or Ordering Document.

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

6. Sub-processors.

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

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

7. Data Transfers

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

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

9. Security Incident Notification. If Motorola becomes aware of a Security Incident, then Motorola must (i) notify Customer of the Security Incident without undue delay, (ii) investigate the Security Incident and apprise Customer of the details of the Security Incident and (iii) take commercially reasonable steps to stop any ongoing loss of Personal Data due to the Security Incident if in the control of Motorola. Notification of a Security Incident must not be construed as an acknowledgement or admission by Motorola of any fault or liability in connection with the Security Incident. Motorola must make reasonable efforts to assist Customer in fulfilling Customer's obligations under Data Protection Laws to notify the relevant supervisory authority and Data Subjects about such incident.

10. Data Retention and Deletion.

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

11. Audit Rights

11.1 Periodic Audit. Motorola will allow Customer to perform an audit of reasonable scope and duration of Motorola operations relevant to the Products and Services purchased under the Agreement, at Customer's sole expense, for verification of compliance with the technical and organizational measures set forth in **Annex II** if (i) Motorola notifies Customer of a Security Incident that results in actual compromise to the Products and/or Services purchased; or (ii) if Customer reasonably believes Motorola is not in compliance with its security commitments under this DPA, or (iii) if such audit is legally required by the Data Protection Laws. Any audit must be conducted in accordance with the procedures set forth in **Section 11.3** of this DPA and may not be conducted more than one time per year. If any such audit requires access to confidential information of Motorola's other customers, suppliers or agents, such portion of the audit may only be conducted by Customer's nationally recognized independent third-party auditors in accordance with the procedures set forth in **Section**

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

11.3 of this DPA. Unless mandated by GDPR or otherwise mandated by law or court order, no audits are allowed within a data center for security and compliance reasons. Motorola must, in no circumstances, provide Customer with the ability to audit any portion of its software, products, and services which would be reasonably expected to compromise the confidentiality of any third party's information or Personal Data.

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

11.3 Audit Process. Customer must provide at least sixty days (60) days prior written notice to Motorola of a request to conduct the audit described in **Section 11.1**. All audits must be conducted during normal business hours, at applicable locations or remotely, as designated by Motorola. Audit locations, if not remote will generally be those location(s) where Customer Data is accessed, or Processed. The audit must not unreasonably interfere with Motorola's day to day operations. An audit must be conducted at Customer's sole cost and expense and subject to the terms of the confidentiality obligations set forth in the Agreement. Before the commencement of any such audit, Motorola and Customer must mutually agree upon the time, and duration of the audit. Motorola must provide reasonable cooperation with the audit, including providing the appointed auditor a right to review, but not copy, Motorola security information or materials provided such auditor has executed an appropriate non-disclosure agreement. Motorola's policy is to share methodology and executive summary information, not raw data or private information. Customer must, at no charge, provide to Motorola a full copy of all findings of the audit.

12. Regulation Specific Terms

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Motorola's possession as may be required under applicable law.

12.3. CJIS. Motorola agrees to support the Customer's obligation to comply with the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy and must comply with the terms of the CJIS Security Addendum for the Term of this Agreement and such CJIS Security Addendum is incorporated herein by reference. Customer hereby consents to allow Motorola "screened" personnel as defined by the CJIS Security Policy to serve as an authorized "escort" within the meaning of CJIS Security Policy for escorting unscreened Motorola personnel that require access to unencrypted Criminal Justice Information for purposes of Tier 3 support (e.g. troubleshooting or development resources). In the event Customer requires access to Service Use Data for its compliance with the CJIS Security Policy, Motorola must make such access available following Customer's request. Notwithstanding the foregoing, in the event the MCA or applicable Ordering Document terminates, Motorola must carry out deletion of Customer Data in compliance with Section 10 herein and may likewise delete Service Use Data within the time frame specified therein. To the extent Customer objects to deletion of its Customer Data or Service Use Data and seeks retention for a longer period, it must provide written notice to Motorola prior to expiration of the 30-day period for data retention to arrange return of the Customer Data and retention of the Service Use Data for a specified longer period of time.

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

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

ANNEX I

A. LIST OF PARTIES

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

1.

Name: …

Address: …

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

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): Controller

2.

…

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

1.

Name: Motorola Solutions, Inc.

Address: …

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

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): Processor

2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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;

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video, and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location, and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified under applicable law or regulation.

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

...

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

Data may be transferred on a continuous basis during the term of the MCA 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 MCA 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 MCA and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities

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

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

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

ANNEX II

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

Measures of pseudonymisation and encryption of personal data

Where technically feasible and when not impacting services provided:

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

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

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

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

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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

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

Measures for user identification and authorisation

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

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

Measures for the protection of data during transmission

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

Measures for the protection of data during storage

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

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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

Measures for ensuring personnel security

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

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

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

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

Measures for ensuring events logging

Protection, and Response. Motorola assesses organization's effectiveness annually via external assessors who report and share the assessment findings with Motorola Audit Services who tracks any identified remediations. For more information, please see the Motorola Trust Center at https://www.motorolasolutions.com/en_us/about/trust-center/security.html

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Measures for certification/assurance of processes and products

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

Measures for ensuring data minimisation

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

Measures for ensuring data quality

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

Measures for ensuring limited data retention

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

Measures for ensuring accountability

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

Measures for allowing data portability and ensuring erasure

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

For transfers to (sub-) processors

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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

ANNEX III

LIST OF SUB-PROCESSORS

1. Microsoft
2. Amazon
3. PagerDuty Inc
4. SalesForce
5. Twilio
6. Neustar
7. Google
8. VMWare
9. CrowdStrike
10. Palo Alto
11. AT&T
12. Okta
13. Cisco
14. Sophos
15. Tenable
16. Corelight

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

NOTICE OF SINGLE OR SOLE SOURCE PROCUREMENT

St Johns County, FL
Purchasing Division
500 San Sebastian View
St. Augustine, FL 32084
Office: (904) 209-0150

Sole/Single Source No: SS No: 1680

Date Posted: January 25, 2024

Written Response due: February 14, 2024

RESPONSES SUBMITTED TO:

Name: Jennifer McDaniel

Email Address: jmcdaniel@sjcfl.us

Phone Number: (904) 209-3270

This is NOT a formal solicitation (RFB, RFP, RFQ) and there are no solicitation documents available. A contract or purchase order is proposed for the product(s) or service(s) identified below. St Johns County, FL, intends to negotiate and award a PO or contract to the Supplier indicated in accordance with Florida State Statute 287.057(5)(c) and 120.57(3). Any responses received as a result of this Notice shall be considered solely for the purpose of determining whether an equivalent product or service can be provided by alternative source(s), which may warrant a competitive solicitation. Responses will NOT be considered as proposals, bids or quotes.

PRODUCT/SERVICE REQUIRED: Cyber Security detection and response solutions for Motorola ASTRO 25 MDR system and PremierOne Managed Detection & Response.

DESCRIPTION: SJC intends to contract with the Vendor to provide Cyber Security needs for our Motorola System.

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

Must provide solution 24x7x365 Security Operations Center Support.

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

- **Included Public Safety Threat Data Feed** — Threat reports covering potential attack vectors based on dark web research. Summaries of actual attacks against public safety and state/local municipalities. Indicator data pulled from a large network of deployed public safety sensors and state/local municipality environments.
- **Advanced Threat Detection & Response** — Consolidate SIEM data and direct threat inputs from endpoint security, network sensors, and cloud/SaaS applications. Pre-built custom playbooks to process alerts and reduce/eliminate manual analyst effort.
- **Single Dashboard for Threat Visibility** — Prioritize based on actual assets in the environment. Asset inventory created manually or automatically with Managed Vulnerability Assessment Service - external and authenticated scans of assets, providing a complete attack surface map.

Chief Information Security Officer (CISO) Benefits
Main dashboard displays and aggregates all of the important and relevant risk information from across the organization, helping decision makers to make better-informed decisions to balance cybersecurity efforts and operational efficiencies.

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

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

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

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

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

PremierOne Managed Endpoint Detection & Response
The ActiveEye Platform

ActiveEye provides event data collection, cloud monitoring and endpoint security automation and remediation across a client's application and security stack. The platform has the ability to give complete visibility into the endpoint, leveraging its machine learning and artificial intelligence to provide a holistic approach to endpoint security. This provides real time endpoint activity data to thwart advanced persistent attacks, while allowing the platform to analyze attacker's behavior and patterns to stop the attacks that have never been seen before. Our solution provides 24x7 Security Operations Center Support. This is a component of our broader proprietary SOC 2 Type 2 certified Managed Security Platform targeted to Public Safety, Critical Infrastructure, and State/Local municipalities.

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

- Included Public Safety Threat Data Feed — Threat reports covering potential attack vectors based on dark web research. Summaries of actual attacks against public safety and state/local municipalities. Indicator data pulled from a large network of deployed public safety sensors and state/local municipality environments.
- Embedded Threat Intelligence — Threat analysts search dark and surface web for intelligence related to attacks against your organization. Identify compromised accounts, phishing attack setups, exposed data, and more specifically related to your organization.
- Integrated Managed Threat Detection & Response — Consolidate SIEM data and direct threat inputs from endpoint security, network sensors, and cloud/SaaS applications. Pre-built custom playbooks to process alerts and reduce/eliminate manual analyst effort.
- Single Dashboard for Threat Visibility — Prioritize based on actual assets in the environment. Asset inventory created manually or automatically with Managed Vulnerability Assessment Service- external and authenticated scans of assets and provides a complete attack surface map.

Chief Information Security Officer (CISO) Benefits

- Main dashboard displays and aggregates all of the important and relevant risk information from across the organization, helping decision makers to make better, informed decisions to balance cybersecurity efforts and operational efficiencies.
- Main dashboard provides key performance metrics and indicators that can inform an admin at a glance to the activity that is occurring throughout their environment.
- Create customize ad-hoc reports and notifications for specific areas of interested to a team.
- Complete transparency into the service that Motorola Solutions is providing. The dashboard will provide the key indicators to the number of events that are handled on a daily, weekly, monthly basis and to how those events are handled by the Motorola SOC.

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

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

INTENDED SOLE/SINGLE SOURCE CONTRACTOR/VENDOR: Motorola Solutions

PROPOSED COST: Total proposed amount over the five (5) year term, $1,505,526.00

PROPOSED CONTRACT/PURCHASE TERM: Five (5) year term.

JUSTIFICATION FOR SOLE/SINGLE SOURCE: Motorola Solutions efficiently meets the cybersecurity Managed Detection and Response needs for the PremierOne system and ASTRO 25 Managed Detection and Response. They are a national and global leader in the cybersecurity community with our recent acquisitions of both Delta Risk and Lunarline in 2020. They have evolved into a holistic mission critical technology provider, placing Information Technology (IT), as well as cybersecurity, at the forefront of importance to protect their customers against threats to the confidentiality, integrity and availability of their operation.

RESPONSE TO SOLE/SINGLE SOURCE:
Suppliers who are capable of providing an equivalent product and/or service as stated herein may submit the following, in writing: Company Name, address, point of contact, contact information (phone #, email, etc.) and statement, description and/or capability to provide an equivalent product/service. Responses shall be submitted to the Point of Contact shown above, by or before the due date provided herein. Responses received after the provided due date shall not be considered.

ATTACHMENTS: N/A

Committee on Military and Veterans Affairs, Space, and Domestic Security

CS/HB 7055 — Cybersecurity

by State Affairs Committee; State Administration and Technology Appropriations Subcommittee; Reps. Giallombardo, Fischer, and others (CS/CS/SB 1670 by Appropriations Committee; Military and Veterans Affairs, Space, and Domestic Security; and Senator Hutson)

The bill amends the state's Cybersecurity Act that requires the Florida Digital Service (FLDS) and the heads of state agencies to meet certain requirements to enhance the cybersecurity of state agencies. Currently, state agencies must provide cybersecurity training to their employees, report cybersecurity incidents, and adopt cybersecurity standards. However, there are no such requirements for local governments.

Current law does not specifically address ransomware, which is a form of malware designed to encrypt files on a device, rendering any files unusable. Malicious actors then demand ransom in exchange for decryption.

CS/HB 7055 prohibits state agencies and local governments from paying or otherwise complying with a ransomware demand.

The bill defines the severity level of a cybersecurity incident in accordance with the National Cyber Incident Response Plan.

State agencies and local governments will be required to report ransomware incidents and high severity level cybersecurity incidents to the Cybersecurity Operations Center and the Cybercrime Office within the Florida Department of Law Enforcement as soon as possible but no later than times specified in the bill. Local governments must also report to the local sheriff.

The bill also requires state agencies to report low level cybersecurity incidents and provides that local governments may report such incidents. State agencies and local governments must also submit after-action reports to FLDS following a cybersecurity or ransomware incident.

CS/HB 7055 requires the Cybersecurity Operations Center to notify the President of the Senate and Speaker of the House of Representatives of high severity level cybersecurity incidents. The notice must contain a high-level overview of the incident and its likely effects. In addition, the Center must provide the President of the Senate, Speaker of the House of Representatives, and the Cybersecurity Advisory Council with a consolidated incident report on a quarterly basis.

The bill requires state agency and local government employees to undergo certain cybersecurity training within 30 days of employment and annually thereafter.

The bill requires local governments to adopt cybersecurity standards that safeguard the local government's data, information technology, and information technology resources.

This summary is provided for information only and does not represent the opinion of any Senator, Senate Officer, or Senate Office.

The bill expands the purpose of the Cybersecurity Advisory Council to include advising local governments on cybersecurity and requires the Council to examine reported cybersecurity and ransomware incidents to develop best practice recommendations. The Council must submit an annual comprehensive report regarding ransomware to the Governor, President of the Senate, and Speaker of the House of Representatives.

The bill creates new criminal penalties and fines for certain ransomware offenses against a government entity.

If approved by the Governor, these provisions take effect July 1, 2022.
Vote: Senate 38-0; House 110-0