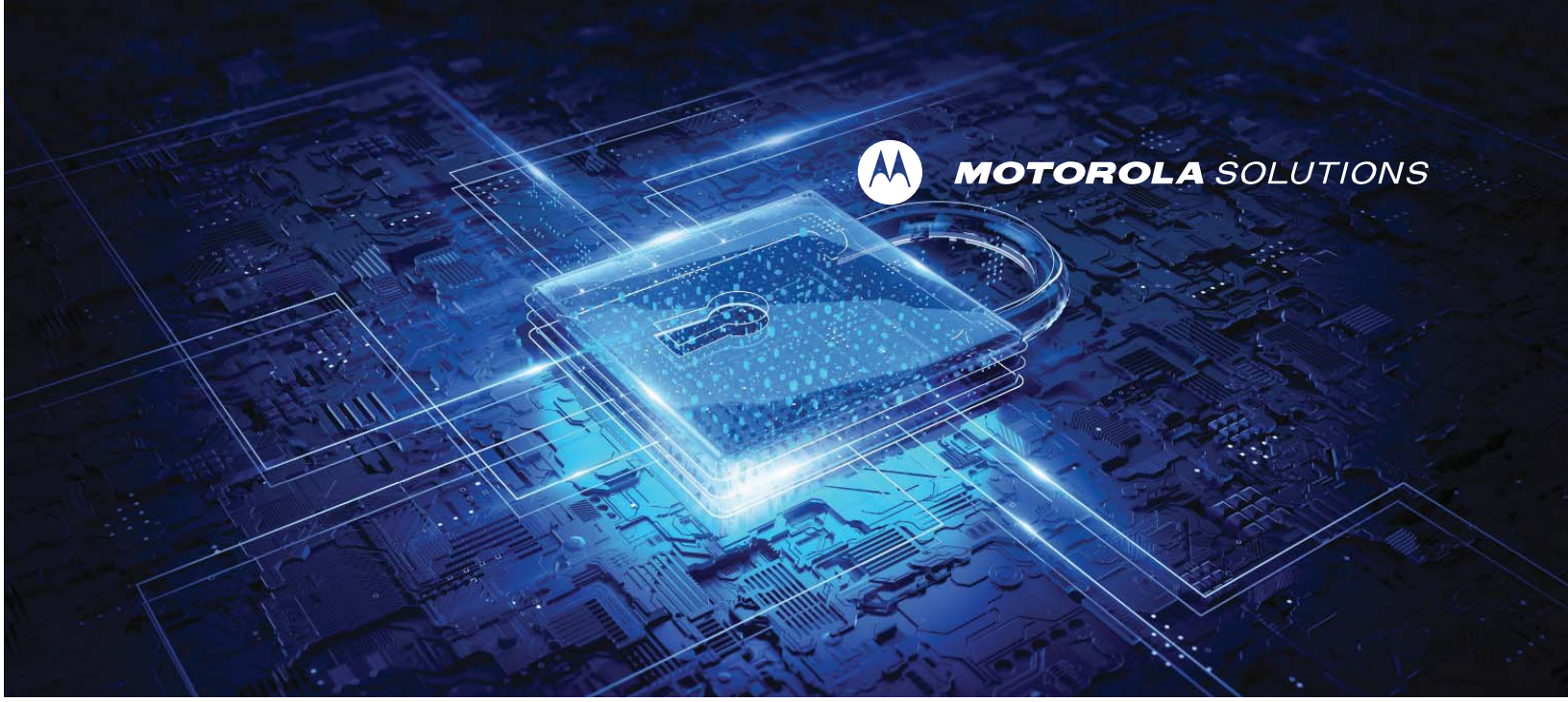


Firm Fixed Price Proposal

Sumter County, FL

ActiveEye Managed Detection & Response

21-127055

December 22, 2021

PS-000127055

Table of Contents

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

December 22, 2021

Stephen Kennedy
Assistant County Administrator, Board of Sumter County Commissioners
7375 Powell Road
Wildwood, Florida 34785

RE: ActiveEye Managed Security Services

Dear Mr. Kennedy,

Motorola Solutions, Inc. (Motorola Solutions) appreciates the opportunity to provide Sumter County, Florida with quality cybersecurity services. Motorola Solutions' project team has taken great care to propose a solution to address your needs and provide exceptional value.

ActiveEye Managed Security Services – Network Monitoring & Endpoint Detection and Response

Motorola Solutions' proposal is conditional upon Sumter County's acceptance of the terms and conditions included in this proposal, or a negotiated version thereof. Pricing will remain valid for thirty (30) days from the date of this proposal.

As required by Sumter County and the state of Florida, Motorola Solutions complies to the following statements:

a. Vendor shall, at all times, comply, to the extent applicable, with the Florida Public Records Law, the Florida Open Meeting Law and all other applicable laws, rules and regulations of the State of Florida.

b. IF THE VENDOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE VENDORS' DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT 352-689-4400, Sumter County Board of County Commissioners, 7375 Powell Road, Wildwood, Florida 34785 or via email at Records@sumtercountyfl.gov.

Any questions Sumter County has regarding this proposal can be directed to Michael Allen, Cybersecurity Account Manager at 518-769-3160 or by email at mike.allen@motorolasolutions.com.

Our goal is to provide Sumter County 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,

Tony McIntosh
MSSSI Vice President & Director of Sales, CyberSecurity

MOTOROLA SOLUTIONS, INC.

Section 1

Executive Summary

Motorola Solutions is pleased to build upon our more than 50 years of ongoing support to Sumter County, FL with a response that efficiently meets the needs for your Enterprise Endpoint Security Threat Management and Response 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.

Motorola Solutions provides VMware Carbon Black as a market leading Next Generation Anti-Virus and Endpoint Detection and Response (NGAV/EDR) platform. The platform is designed to bring the most sophisticated threats and alerts to the cybersecurity analysts to provide quick, easy access to the information that is needed to resolve, remediate and strengthen the endpoint security posture. Our Endpoint Security Threat Management Solution provides a Co-Managed Security Orchestration, Automation and Response (SOAR) platform known as ActiveEye (AE).

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.

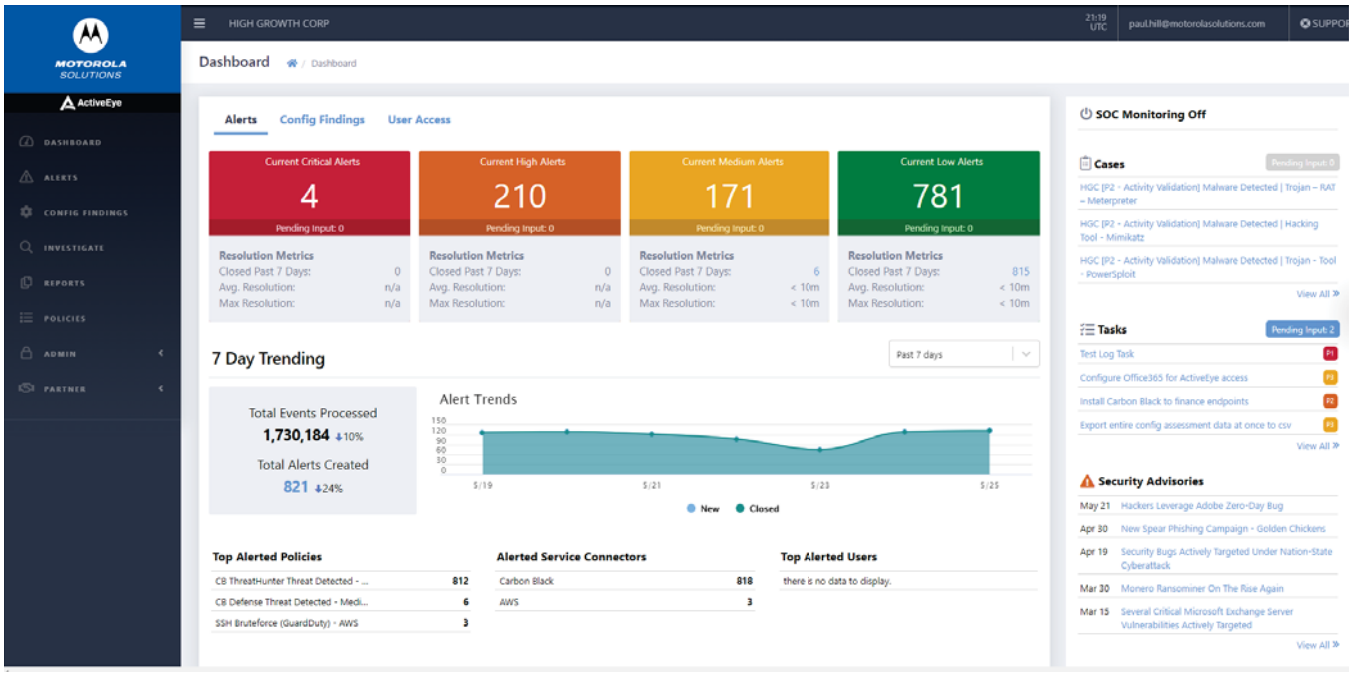
The ActiveEye Platform

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

- Included Public Safety Threat Data Feed — Threat reports covering potential attack vectors based on dark web research. Summaries of actual attacks against public safety and state/local municipalities. Indicator data pulled from a large network of deployed public safety sensors and state/local municipality environments.
- 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

The ActiveEye Managed Security dashboard can be seen below:



Benefits for Sumter County

- 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

- 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.

WHY MOTOROLA SOLUTIONS

Company Background and History

Motorola Solutions 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 more 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 Solutions brand.

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

Motorola Solutions connects people through technology. Public safety and commercial customers around the world turn to Motorola Solutions 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 Solutions' 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 ("Motorola") is pleased to present this budgetary proposal of cyber security services for Sumter County, FL (hereinafter referred to as "Customer").

The following cyber security services are included in our proposal:

- **ActiveEye℠ Managed Detection & Response**. The following service modules are included:
  - Log Analytics
  - Network Detection
  - Endpoint Detection and Response
    - VMware Carbon Black Cloud Enterprise EDR (Threat Hunter)
- **Motorola Security Operations Center (SOC) Monitoring and Support**

2.2 Services Included

The ActiveEye service modules included in our proposal are selected in the **Subscribed** column below.

Table 2-1. Service Modules

Service Module	Features Included	Subscribed
ActiveEye Remote Security Sensor (AERSS)	Number of sensors: 1	X
Log Analytics	500 GB/Month Online Storage Period: 30 Day Storage Extended Log Storage Length: 12 Months	X
Network Detection	1 Gbps monitored across all sensors	X
Endpoint Detection and Response (EDR)	Carbon Black Defense + Threat Hunter 100 EDR Total Endpoints Online Storage Period: 30 Day Storage	X

The Motorola SOC services included in our proposal are selected in the **Subscribed** column below.

Table 2-2. Motorola SOC

Motorola SOC	
Motorola SOC 24x7	X

2.3 Service Description

The ActiveEye platform collects and manages security data, optimizing threat detection and increasing focus on the most critical alerts that require quick responses. Built-in analytics examine multiple real-time threat intelligence feeds, reference past events, and follow defined playbooks to automate most analyst actions. Analytics also rank manual investigations, prioritizing those most likely to require remediation.

ActiveEye can integrate a variety of components to gather data, including a security information and event management (SIEM) tool. ActiveEye conveys processed data from these components to the Customer and Motorola in the ActiveEye Managed Security Portal. In addition, ActiveEye Portal displays source data collected from network elements.

Security Orchestration, Automation, and Response

As a SOAR platform, ActiveEye orchestrates the flow of data and actions, speeding remediation by automatically performing investigation and response tasks. Using predefined or custom playbooks, ActiveEye handles repetitive and precise tasks in place of human SOC analysts. ActiveEye supports two types of automation:

- Investigation Automation - Using playbooks, ActiveEye can look up threat intelligence, query past data, add recommended action notes to cases, and surface event details to the main investigation screen. Before an analyst views an alert, ActiveEye collects key event data for their review.
- Response Automation - ActiveEye can take response actions defined in playbooks. Actions can include changing alert priority, closing an alert, blocklisting files, removing files from systems, or isolating a host from the network.

This automation gets key event data to SOC analysts sooner, and bypasses manual steps for time-sensitive response tasks. With ActiveEye, SOC analysts can shift their focus to more complex investigation and response tasks.

Log Collection and Archive

Compiling log information from multiple sources makes it easier to manage large volumes of security data. To enable comparison and analysis of data from across the network, ActiveEye normalizes log data and enriches it with data from multiple sources.

ActiveEye also retains the raw log data of every event so analysts can review other event attributes if needed. Past log data is classified into two groups to make it easier to access more recent and relevant data:

- Short Term Storage - Contains security logs for a default period of 30 days, or for custom configured period of up to 90 days. Logs in short term storage are available for simple query, since they are the most likely to be accessed during security incident investigations.
- Long Term Archive - Stores security logs for a default of 1 year, or for up to 7 years. Long term archives preserve historical data to meet compliance regulations, and to support investigations and threat hunts.

ActiveEye can collect logs from cloud-based services, as well as data centers or on-premises components. Cloud-based services - such as Carbon Black, Crowdstrike, Okta, Office365, and Amazon Web Services - send logs directly to the ActiveEye platform using secure APIs. Log sources in data centers or on Customer's premises will use the ActiveEye Remote Security Sensor to aggregate logs and securely forward them to ActiveEye for analysis and archiving.

ActiveEye Remote Security Sensor

ActiveEye Remote Security Sensors integrate the ActiveEye platform with network elements, enabling it to collect logs from syslog, as well as analyze network traffic over span port connections and scan elements for vulnerabilities. Motorola deploys these sensors as a hardware component.

Software as a Service Platform

As a cloud service, ActiveEye is quick and simple to deploy, removing the burden of installing, maintaining, and managing an on-premises SIEM. Depending on the log sources that need to be monitored, ActiveEye can replace the need for any separate SIEM component.

ActiveEye access and content are protected by powerful security functions. Users access the platform via a secure web browser using multi-factor authentication. Administrative functions will enable the Customer to manage user access as needed. The platform undergoes regular security audits and has an active SOC 2 Type2 audit certification.

2.3.1 ActiveEye Portal

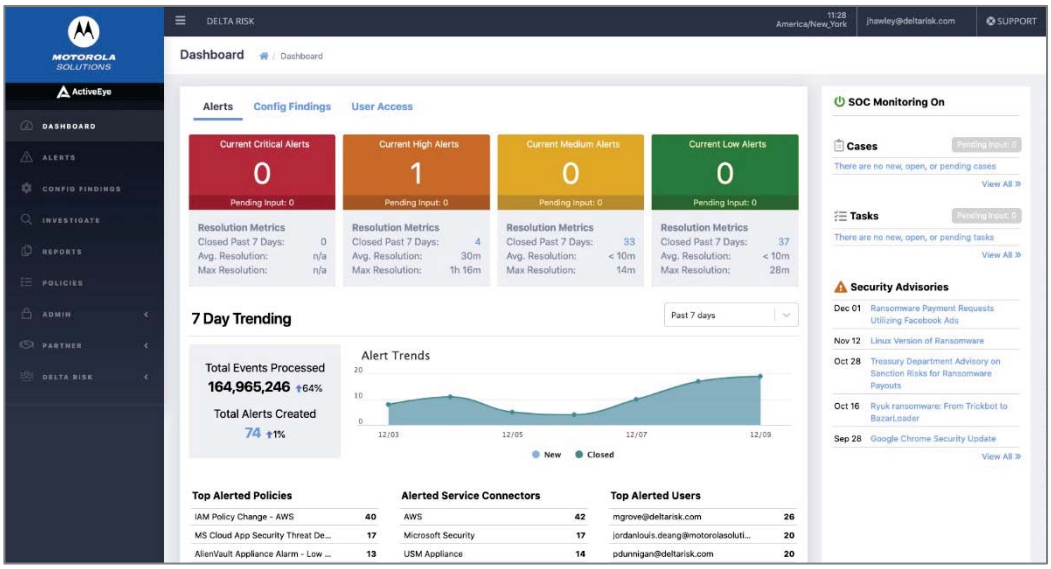


Figure 2-1. ActiveEye Interface

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

Dashboard

Key information in the ActiveEye Portal is summarized on the dashboard. This dashboard includes open alerts, an overview of alert categories, alert processing key performance indicators (KPI), open security cases, and recent threat advisories. From here, 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 creates a security case. Through the ActiveEye Portal, the Customer can view details of current or past cases, create new cases, or respond to ongoing cases.

Alert Details and Trends

Alerts are system notifications of unusual activity. These alerts can be evidence of a past, active, or developing threat. If analysts believe alerts are indicative of a threat, they can open security cases based on them.

ActiveEye records relevant data for each alert, enabling users to quickly view its triggers, systems it impacts, and any actions taken to address it. Each alert record also includes a summary of key attributes. From that alert summary, users can access related records for more details. These records include threat intelligence, past event data, related events, and activity logs.

To put alerts into context, ActiveEye Portal provides tools for reviewing groups of alerts based on key attributes or time periods. Attribute filters enable users to toggle which alert groups ActiveEye Portal shows, helping to spot trends or threat activity. Users can also compare alert logs for specific time periods to determine if specific trends are associated with a threat or are false positives.

Investigations and Reporting

ActiveEye Portal's robust ad hoc reporting capabilities enable users to investigate and hunt active threats, and to view historical data sets. Reports provide a simple, consistent view of collected event data. Pre-defined templates organize the data and display the most important attributes of event types. Users can customize these standard reports to display and summarize different attributes when needed. To share information outside of ActiveEye Portal, users can download reports in .csv or .json format. Downloaded reports may contain a maximum of 50,000 rows.

In addition to ad hoc reporting and querying, ActiveEye Portal can provide a monthly report and a daily email summary if needed. The monthly report summarizes important security items for the month, and is available as a PDF download. The daily email summary provides a customized set of statistics from the previous day to a predetermined user list. This summary can include alert counts, security cases opened/closed, saved queries that have new data, and detailed endpoint security statistics. ActiveEye Portal can send one or more summary emails with different content for different groups.

Security Advisories

Security Advisory messages from the SOC 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

To support effective security management, ActiveEye Portal includes several functions for sharing information. Automatic security alerts notify defined contacts of incidents based on incident priority. In addition to automatic security alerts, ActiveEye Portal features other information sharing functions that the Customer and Motorola can access:

- 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 that the SOC will consult 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.

Together, these functions quickly spread important information to security teams and analysts.

User Access

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

2.3.2 Service Modules

ActiveEye delivers service capability by integrating one or more service modules. With more modules, ActiveEye analytics receive 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.

Service module options are separately licensed components that integrate different aspects of the Customer security and IT infrastructure. Each module integrates direct monitoring or third-party systems into ActiveEye, enabling visibility, orchestration and automation from one platform.

As an option, the Customer can integrate supported components into the ActiveEye service via Service Connectors available from Motorola. Motorola maintains and continually updates a library of Service Connectors.

The following subsections describe the service modules selected in **Table 2-1.** Service Modules.

2.3.2.1 ActiveEye Remote Security Sensor

ActiveEye Remote Security Sensors (AERSS) integrate the ActiveEye platform with network elements, enabling it to collect logs from syslog, as well as analyze network traffic over span port connections and scan elements for vulnerabilities.

AERSS will be deployed into the ASTRO 25 network and applicable CEN systems to deliver the service. These sensors monitor geo diverse sites in the system for security events and pass security information to the ActiveEye platform.

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

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

2.3.2.2 Log Analytics

The Log Analytics function collects log data from systems, applications, networking components, security systems, and even other SIEM solutions. Several analytics components and security policies process log data to identify policy violations and suspicious activity. If ActiveEye detects an event of interest that may represent a threat, it will alert analysts based on Customer's settings.

Over time, past logged events can provide critical context to track the origin of a threat or identify a new threat using previous attack patterns. ActiveEye stores collected events so analysts can search through them and use them for threat hunting. Events remain in storage for a defined period of time based on subscription. The default term is one year. Longer time periods are available for subscription.

ActiveEye can incorporate logs from a variety of systems. These include authentication and authorization systems, object storage, cloud virtual networks, virtual servers, cloud security services, software applications, and physical infrastructure.

The Customer may deploy one or more ActiveEye Remote Security Sensors to collect logs.

Collected events will be stored in the ActiveEye 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 2-1.** Service Modules for subscription details.

2.3.2.3 Network Detection

The Network Detection service module automates the investigation of network traffic alerts and allows security teams to view those alerts in the context of other user activity. To enable this feature, the ActiveEye Intrusion Detection System (IDS) is deployed within Customer's network to perform real time signature and anomaly detection. The IDS analyzes traffic for signs of malicious activity in real time. In addition, the IDS performs packet level and flow level analysis, enabling network communications modeling. This information is used to identify anomalous behavior that is not captured by pre-defined traffic signatures, including activity over encrypted connections.

The Network Detection service is enabled by one or more ActiveEye Remote Security Sensors to perform traffic analysis.

2.3.2.4 Endpoint Detection and Response

ActiveEye Managed Endpoint Detection and Response (EDR) integrates market leading EDR tools with the ActiveEye platform to provide additional threat intelligence, automated investigation, and orchestrated response actions to optimize protection of critical systems.

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

The platform enables analysts to initiate response actions (i.e. isolate host, block list a file, allow list a file, and remove file) on endpoints to respond to detection of verified malicious activity within the Customer's system. Available responses are determined by the Customer's EDR tool and security policies.

The license for the EDR solution may be included with this service if not already procured by the Customer. See **Table 2-1.** Service Modules for subscription details.

2.3.3 Security Operations Center Monitoring and Support

Motorola's Security Operations Center (SOC) will monitor ActiveEye connected networks, applications and devices for security threats 24/7. Based on their broad security experience, the SOC's analysts will

recommend security device configurations that optimize threat detection and implement playbooks to increase focus on the most critical threats.

If a threat investigation requires input from the Customer security contacts, the SOC will create a Security Case and follow predefined escalation procedures for each priority level. If the SOC cannot make contact with the first level, the SOC will escalate as defined. The ActiveEye Portal will enable the Customer to view security cases and event investigation history.

In the event of a potential incident, the SOC will use data available in ActiveEye and access the Customer's system to determine the extent of malicious activity. If needed, the SOC will add more detection policies to the Customer's Service Modules. With the EDR service module, the SOC can take mitigating actions on remote hosts systems based on a pre-approved response plan, or if they determine it to be necessary for a specific case. When needed, the SOC will recommend mitigating actions the Customer can take to address a threat.

The SOC team operates from secure, redundant locations in the United States. The teams can securely operate at remote locations if needed. The teams complete regular training on customer data management and privacy to protect sensitive customer data.

Section 3

Statement of Work

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 ("Motorola") Cyber Security services as presented in this proposal to Sumter County, FL (hereinafter referred to as "Customer").

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

3.1 Deployment Timeline and Milestones

To initiate the ActiveEye Managed Detection & Response service ("the Service"), Motorola and the Customer must perform deployment tasks. Deployment of the Service is broken into the following phases, each with specific deliverables.

Phase 1: Information Exchange

Motorola Responsibilities: Motorola will schedule a service kick-off meeting with Customer and provide information-gathering documents to Customer within one week of contract signature. The kick-off meeting may be conducted either remote or in-person, at the earliest mutually available opportunity.

Customer Responsibilities: Customer must attend the kick-off meeting and complete information gathering documents as quickly and accurately as possible. Failure to do so will delay the accomplishment of future phases.

Phase 2: Infrastructure Readiness

Motorola Responsibilities: Motorola will provide detailed requirements regarding customer infrastructure preparation actions within one week of the kick-off meeting.

Customer Responsibilities: Customer must accomplish all infrastructure preparation tasks as quickly as possible. Failure to do so will delay the accomplishment of future phases.

Phase 3: System Buildout and Deployment

Motorola Responsibilities: 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. Motorola will accomplish these within one-week of the completion of all infrastructure readiness tasks.

Customer Responsibilities: Customer must deploy tools, as applicable, in their environment, in accordance with provided requirements. Failure to do so will delay the accomplishments of future phases.

Phase 4: Monitoring Turn Up

Motorola Responsibilities: Motorola will monitor the service and ensure all in-scope assets are properly forwarding logs or events. Motorola will notify the customer of any exceptions. Motorola will begin monitoring any properly connected in-scope sources after the initial tuning period.

Customer Responsibilities: The customer must ensure appropriate connectivity for all in-scope assets to the service and address any exceptions noted by Motorola. Failure to do so will delay the accomplishment of future phases and will prevent Motorola from monitoring those sources.

Phase 5: Tuning/Report Setup

Motorola Responsibilities: Motorola will conduct initial tuning of the events and alarms in the Service, as well as set up initial reports (User Access, Administration Events, and Configuration Findings Reports).

Customer Responsibilities: The Customer must deploy tools, as applicable, in their environment, in accordance with provided requirements. The Customer must engage the Security Operations Center (SOC) team in discussing the tuning approach and confirm the configurations requested.

3.2 ActiveEye Platform

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

Motorola Responsibilities

- Provide access to the ActiveEye portal for the Customer and any identified, approved users. After initial deployment, the Customer will have self-service access to add/remove/update user access as needed.
- Provide the services subscribed to, as noted in Table 2-1. Service.
- Provide ActiveEye Remote Security Sensor hardware or virtual appliance.
- Provide remote setup and configuration assistance of ActiveEye Remote Security Sensor.
- Provide ActiveEye Remote Security Sensor system software updates as needed
- Make monthly services implementation and status reports available to the Customer.
- Resolve platform issues and technical errors as documented by the Customer.
- Retain security logs within ActiveEye. Security logs will be retained for the length of time designated by the long-term storage policy selected by the Customer.
- Configure ActiveEye for log sources (from security devices and other high-value assets) per the scope of the subscribed service modules.

Customer Responsibilities

- Provide reasonable assistance to Motorola to perform the Service, as described in this SOW. This assistance includes, but is not limited to, technical assistance with issues that may require physical access to the devices affected by this Service, or virtual assistance with virtual environment issues that require administrative access to devices affected by this Service.
- Provide all technical, license, and service information requested in the implementation documents prior to the commencement of the Service.

- Perform all network and system integrations necessary for ActiveEye Service. This includes providing external connectivity for ActiveEye security components.
- Install agents on in-scope systems and devices, as required.
- Configure all necessary components of Customer's infrastructure to integrate with ActiveEye.
- Provide the name, email, landline telephone numbers, and mobile telephone number for all shipping, installation, and security Points of Contact (POC)s.
- Manage user access to the ActiveEye portal, creating new user accounts when needed and removing a user's access when it is no longer required.

3.2.1 Service Modules

The following subsections describe the delivery of the service modules selected in **Table 2-1.** Service Modules.

3.2.1.1 Log Analytics

The ActiveEye platform will continuously monitor for events of interest and alerts generated by integrated components, and cross-correlate them with other information within the platform. The Customer can configure customizable alerts and notifications for detected security events.

Motorola Responsibilities

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

Customer Responsibilities

- Configure networking infrastructure to allow ActiveEye Remote Security Sensor to communicate with ActiveEye as defined.
- Configure log sources or on-premises security information and event management (SIEM) solution to either enable ActiveEye to authenticate to the system or configure log sources to be forwarded to ActiveEye.

3.2.1.2 Network Detection

ActiveEye Network Detection enables security teams to automate investigation of network alerts and view this activity in the context of other user activity.

Motorola Responsibilities

- Work with the Customer to integrate ActiveEye Remote Security Sensor(s) containing the Network Intrusion Detection System into the Customer's system.

Customer Responsibilities

- Configure networking infrastructure to allow ActiveEye Remote Security Sensor to communicate with ActiveEye as defined.
- Configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a SPAN port on a switch) network traffic to the ActiveEye sensor.

3.2.1.3 Endpoint Detection and Response

Motorola Responsibilities

- Work with the Customer to integrate ActiveEye Service Connector(s) necessary to monitor and interact with the Customer's Endpoint Detection and Response (EDR) solution.

Customer Responsibilities

- Deploy and maintain EDR agents to required systems.
- Configure networking infrastructure to allow EDR agents to communicate with centralized server components.
- Configure EDR solution to enable ActiveEye connection for event/alert collection and response actions.

3.2.2 Technical Support

ActiveEye Managed Detection & Response Technical Support provides the Customer with a toll-free telephone number and email address for ActiveEye Managed Detection & Response support requests, available Monday to Friday from 8am to 7pm CST. Support requests are stored in a ticketing system for accountability and reporting.

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 platform and does not include use or implementation of third-party components.

3.3 Security Operations Center Monitoring and Support

Motorola's Security Operations Center (SOC) will provide continuous 24x7 monitoring through automated tools and review by trained security analysts. Motorola will analyze events and notify the Customer in accordance with **Table 3-2.** Notification Procedures.

Motorola will start monitoring the Service in accordance with Motorola processes and procedures after deployment, as described in Section 3.1 Deployment Timeline and Milestones.

The SOC receives system-generated alerts 24/7, and provides the Customer with a toll-free telephone number and email address for support requests, available 24/7. Support requests are stored in a ticketing system for accountability and reporting.

3.3.1 Ongoing 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
- Attempt to determine the root cause and extent of compromise using existing monitoring capabilities in place as part of the 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 Network Map detailing the Customer's network architecture for network(s) in scope for the Service, if available.
- Provide a timely response to SOC security incident tickets or investigation questions.
- Provide an established service window in which qualified IT personnel will be able to respond to major event escalations.
- Notify Motorola at least twenty-four (24) hours in advance of any scheduled maintenance, network administration activity, or system administration activity that would affect Motorola's ability to perform the Managed SOC Service, as described in this SOW.

3.3.2 Service Module Specific SOC Services

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

The following describe these security operations modules.

3.3.2.1 Managed Log Analytics

Motorola SOC will consult with the Customer to identify log sources for the level of threat detection desired in each environment.

The SOC will, on a regular basis, advise the Customer on recommendations for each log source type that will optimize storage and visibility to actual threats.

Motorola Responsibilities

- Consult with and advise the Customer on performing necessary system configurations to optimize log volumes and content.

Customer Responsibilities

- Update log source configurations as necessary to optimize log content and volume sent to ActiveEye platform.

3.3.2.2 Managed Network Detection

Motorola's SOC will consult with Customer on the deployment of the Network Detection Service components.

The SOC will continually 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.

Motorola Responsibilities

- Optimize the policies and configurations to tune out noise and highlight potential threats.

Customer Responsibilities

- Initiate recommended response actions when active attacks are detected.

3.3.2.3 Managed Endpoint Detection and Response

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

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

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

Motorola Responsibilities

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

Customer Responsibilities

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

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

3.3.3.1 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.

3.3.3.2 Tuning

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

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

3.3.3.3 Tuning Period Exception

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

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

3.3.4 Limitations and Exclusion

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

3.4 Scope Limitations & Clarifications

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 proposal. 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.

Customer and Third-Party Information

The 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 purposes of this engagement, so long 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, 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.

Section 4

Proposal Pricing

4.1 Pricing Summary

Motorola pricing is based on the services presented. The addition or deletion of any component(s) may subject the total solution price to modifications.

The following table describes annual recurring payments for managed security services:

Product Description	Service Setup Cost (One-time Fee)	Annual Service Cost
ActiveEye℠ Managed Detection and Response includes SOC services – Year 1	$15,127	$132,762
Initial Subscription Period Year 1 (Due at Signing):		**$147,888**
Initial Subscription Period Year 2 (Optional):		**$152,325**

4.2 Payment Schedule & Terms

Period of Performance

The initial subscription period of the contract will extend twelve (12) months from the Commencement Date of Service, defined as the date data is available for analysis, or not later than thirty (30) days after Motorola provides the Customer with necessary hardware or software to connect the first data source.

Term

The Term of the contract begins on the Commencement Date of Service and remains in effect until the expiration of the initial period so specified. Upon expiration of the initial term, the Service will automatically renew for additional periods of one (1) year unless one Party provides the other written notice that it is terminating such Service not less than sixty (60) days prior to the end of the Term then in effect.

Billing

Upon acceptance of this proposal by the Customer, Motorola will invoice the Customer upon the execution of this proposal for all service fees in advance for the full annual amount according to the Pricing table in Section 4.1 Pricing Summary.

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.

Tax

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

Section 5

Contractual Documentation

Cyber Addendum

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

Section 1. APPLICABILITY

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

Section 2. ADDITIONAL DEFINITIONS AND INTERPRETATION

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

2.2 "Customer Data" means Customer data, information, and content, provided by, through, or on behalf of Customer, its Authorized Users, and their end users through the use of the Services. Customer Data does not include Customer Contact Data, Service Use Data, or information from publicly available sources or other Third-Party Data or Motorola Data or anonymized or generalized data. For avoidance of doubt, so long as not specifically identifying the Customer, Customer Data shall not include, and Motorola shall be free to use, share and leverage security threat intelligence and mitigation data generally, including without limitation, third-party threat vectors and IP addresses, file hash information, domain names, malware signatures and information, information obtained from third-party sources, indicators of compromise, and tactics, techniques, and procedures used, learned or developed in the course of providing Services.

2.3 "Feedback" means comments or information, in oral or written form, given to Motorola 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.

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

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

2.6 "Service Use Data" means data generated by Customer's use of the Services or by Motorola's support of the Services, including personal information, threat data, security threat intelligence and mitigation data, vulnerability data, threat scenarios, malicious and third-party IP information, malware, location, monitoring and

recording activity, product performance and error information, threat signatures, activity logs and date and time of use.

2.7 "Statement(s) of Work" or "SOW(s)" as used in this Addendum means a statement of work, ordering document, accepted proposal, or other agreed upon engagement document issued under or subject to this Addendum. Mutually agreed upon SOWs may be attached hereto as Exhibit(s) A-1, A-2, A-3, etc., and/or are respectively incorporated by reference, each of which will be governed by the terms and conditions of this Agreement. 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 Agreement. The Deliverables, if any, are more fully described in the Statements of Work.

2.8 "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.

Section 3. LICENSE, DATA AND SERVICE CONDITIONS

3.1 Delivery of Cyber Services

3.1.1 All Professional Services will be performed in accordance with the performance schedule included in a Statement of Work ("SOW"). Delivery of hours purchased as Retainer Services is at the onset of the applicable retainer period. Hours purchased as Retainer Services expire and are forfeited if not used within the Retainer period, subject to terms of use, expiration and extension, if any, as set out in the applicable SOW or ordering document. Professional Services described in a SOW will be deemed complete upon Motorola'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 Services or upon Motorola otherwise providing access to the 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 Motorola Materials. Motorola grants Customer and Authorized Users a limited, non-transferable, non-sublicenseable, and non-exclusive license to use the Services and associated deliverables solely for Customer's internal business purposes.

3.3 To the extent Customer is permitted to access, use, or integrate Customer or third-party software, services, content, or data that is not provided by Motorola (collectively, "Non-Motorola 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 Section 3.5 – Processing Customer Data, below. The Parties agree that with regard to the Processing of personal information which may be part of Customer Data, Customer is the controller and Motorola is the processor, and Motorola may engage sub-processors pursuant to Section 3.5.3 – Sub-processors and Third-Party Providers.

3.5 Processing Customer Data.

3.5.1. Motorola 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 Addendum, (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 Addendum, along with any related 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.

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

3.5.3 Sub-processors and Third-Party Providers. Motorola 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. Notwithstanding any provision to the contrary, to the extent the use or performance of certain Services is governed by any separate license, data requirement, EULA, privacy statement, or other applicable agreement, including terms governing third-party software, hardware or services, including open source software, Customer will comply, and ensure its Authorized Users comply, with any such agreements or terms, which shall govern any such Services.

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

3.6 Service Use Data. Customer understands and agrees that Motorola 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, 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.

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

3.8. Third-Party Data and Motorola Data. Motorola Data and Third-Party Data may be available to Customer through the Services. Customer will not, and will ensure its Authorized Users will not: (a) use the Motorola Data or Third-Party Data for any purpose other than Customer's internal business purposes; (b) disclose the data to third parties; (c) "white label" such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (d) use such data in violation of applicable laws; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data; or (f) modify such data or combine it with Customer Data or other data or use the data to build databases. Any rights granted to Customer or Authorized Users with respect to Motorola Data or Third-Party Data will immediately terminate upon termination or expiration of this Addendum. 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 Addendum, 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 this Addendum and the Primary Agreement to the contrary, Motorola will have no liability for Third-Party Data or Motorola Data available through the Services. Motorola and its Third-Party Data providers reserve all rights in and to Motorola Data and Third-Party Data.

3.9 Customer will ensure its employees and Authorized Users comply with the terms of this Addendum and will be liable for all acts and omissions of its employees and Authorized Users. Customer is responsible for the secure management of Authorized Users' names, passwords and login credentials for access to products and Services. "Authorized Users" are Customer's employees, full-time contractors engaged for the purpose of supporting the products and Services that are not competitors of Motorola 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.

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

3.11 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 4. WARRANTY

4.1 CUSTOMER ACKNOWLEDGES, UNDERSTANDS AND AGREES THAT MOTOROLA DOES NOT GUARANTEE OR WARRANT THAT IT WILL DISCOVER ALL OF CUSTOMER'S SECURITY EVENTS (SUCH EVENTS INCLUDING THE UNAUTHORIZED ACCESS, ACQUISITION, USE, DISCLOSURE, MODIFICATION OR DESTRUCTION OF CUSTOMER DATA), THREATS, OR SYSTEM VULNERABILITIES. MOTOROLA 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. Motorola disclaims responsibility for costs in connection with any such disruptions of and/or damage to Customer's or a third party's information systems, equipment, voice transmissions, data and Customer Data, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision or delivery of the Service.

4.3. Motorola warrants that Supplied Equipment, under normal use and service, will be free from material defects in materials and workmanship for one (1) year from the date of shipment, subject to Customer providing written notice to Motorola 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. 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 express warranties provided by such third parties.

Section 5 LIMITATION OF LIABILITY

5.1. DISCLAIMER OF CONSEQUENTIAL DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, MOTOROLA, 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 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 CYBER SERVICES UNDER WHICH THE CLAIM AROSE. NOTWITHSTANDING THE FOREGOING, FOR ANY SUBSCRIPTION 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 CYBER SERVICES TO WHICH THE CLAIM IS RELATED DURING THE CONSECUTIVE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT FROM WHICH THE FIRST CLAIM AROSE. FOR AVOIDANCE OF DOUBT, THE LIMITATIONS IN THIS SECTION 5.2 APPLY IN THE AGGREGATE TO INDEMNIFICATION OBLIGATIONS ARISING OUT OF THIS ADDENDUM OR ANY RELATED AGREEMENTS.

5.3. ADDITIONAL EXCLUSIONS. NOTWITHSTANDING ANY OTHER PROVISION OF THIS ADDENDUM, THE PRIMARY AGREEMENT OR ANY RELATED AGREEMENT, MOTOROLA 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.

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

In witness whereof, the Parties hereto have executed this Addendum as of the Effective Date.

MOTOROLA	CUSTOMER
BY: _____	BY: _____
NAME: _____	NAME: _____
TITLE: _____	TITLE: _____
DATE: _____	DATE: _____