STATE OF NORTH CAROLINA

COUNTY OF GUILFORD

Amendment No 16 to Guilford County Contract No. 36460-04/95-211
for 800 MHz Radio System

THIS AGREEMENT is hereby made and entered into this 1st day of July, 2025 by and between GUILFORD COUNTY, on behalf of its Emergency Services Department, hereinafter referred to as the "COUNTY," and the CITY OF GREENSBORO, on behalf of its Technical Services Division, hereinafter referred to as the "CITY," and also collectively referred to as the "PARTIES."

W I T N E S S E T H :

WHEREAS, The CITY and COUNTY have collaborated in a joint Public Safety Radio System since 1995 to benefit the communications of public safety responders, and have determined that there are mutual interests and advantages for the COUNTY and CITY to maintain this relationship; and,

WHEREAS, the CITY and COUNTY desire to reaffirm their commitment to a shared ownership Agreement through promulgation of this new Amendment to an existing Interlocal Agreement; and,

WHEREAS, the PARTIES reaffirmed their ownership interests in a multitude of amendments, the most recent of which was Amendment #15 hereto, which was executed in July 1, 2023 and,

WHEREAS, the COUNTY and the CITY mutually desire to assure that the radio infrastructure is maintained in a high state of readiness and on current technology platforms; and,

WHEREAS, to do so, the PARTIES need to address two new contracts needed to maintain and enhance system functionality and security (one with Motorola and one with PCTEL) and to address those new contracts by this Amendment No. 16 while otherwise continuing their collaboration on the terms of the existing Interlocal Agreement, as previously amended; and,

WHEREAS, pursuant to the authority of Chapter 160A, Article 20, Section 461 *et seq.* of the North Carolina General Statutes, the Parties are authorized to enter into this Interlocal Agreement in order to pursue the above stated goals;

NOW, THEREFORE, for the purpose and subject to the terms and conditions hereinafter set forth, it is hereby agreed as follows:

The following new paragraphs are added to the Interlocal Agreement as previously amended:

26. Attachment I is the FY26 through FY28 maintenance agreement with Motorola for enhanced cybersecurity. COUNTY agrees to pay 50% of the costs incurred pursuant to this agreement. For the three year term, this amount shall not exceed $102,633.14 total and shall not exceed the following amounts by year: $59,486.73 FY26, $21,150.20 FY27, and $21,996.21 FY28, with payments divided as outlined in the attachment. COUNTY agrees to annual installment payments to CITY upon being billed.

27. Attachment J is the FY26 through FY28 agreement with PCTEL for maintenance of the PARTIES' respective See Hawks. COUNTY agrees to pay 50% of the costs incurred pursuant to this agreement. For the three year term, this amount shall not exceed $40,807.94 and shall not exceed $13,602.65 per annum, with payments divided as outlined in the attachment. COUNTY agrees to annual installment payments to CITY upon being billed.

28. Attachment K is a summary of all known costing of system maintenance and monitoring agreements for the system for the term of this agreement to align to FY26-FY28, as well as the costing for the Motorola SUAII for FY29 and Managed Detection and Response Services for FY29 and FY30.

All other provisions of Contract No. **36460-04/95-211** and its Amendments, are hereby ratified and shall continue in full force and effect without change, unless and until revised upon mutual written Agreement of the Parties, or terminated as provided herein.

(The remainder of this page has been intentionally left blank.
The contract continues, including signatures, on the following page.)

IN WITNESS WHEREOF, the COUNTY and CITY have set their hands and seals as of this day and year first above written.

GUILFORD COUNTY

_____
Erris Dunston Date
Guilford Assistant County Manager

ATTEST:

_____
Robin B. Keller Date
Guilford County Clerk to Board

(COUNTY SEAL)

APPROVED AS TO CONTENT:

_____
James L. Albright, Director Date
Guilford County Emergency Services

(The remainder of this page has been intentionally left blank.
The Contract continues, including signatures, on the following page.)

Recommended by: _____
Melanie Jones
Executive Director, Guilford Metro 911

Recommended by: _____
Lewis Cheatham
Technical Services Manager, Guilford Metro 911

CITY OF GREENSBORO

_____
Nathaniel Davis or designee
Greensboro City Manager

ATTEST:

_____
Greensboro City Clerk

(CITY SEAL)

This instrument has been pre-audited in the manner required by the Local Government Budget and Fiscal Control Act.

_____
Greensboro City Finance Officer

APPROVED AS TO FORM:

_____
Charles Watts
Greensboro City Attorney

Attachment I

Insert Motorola contract

City of Greensboro

Managed, Detect & Respond Core & CEN

Amanda Pruett **404.430.7162** **amanda.pruett@motorolasolutions.com**

Table of Contents

Solution Summary

ASTRO MDR		
Standalone (ASTRO 25)	✔	Provides access to the ActiveEye Security Platform, along with 24/7 support from specialized cybersecurity experts who monitor mission-critical ASTRO systems for indicators of threats. This is for standalone ASTRO systems, including a core.

Executive Summary

Motorola is pleased to build upon our years of ongoing support to City of Greensboro with a response 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.

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. In addition to the intelligence alerts and reports provided, other benefits included access to an automated threat feed, with context and tags, that can be fed into your SIEM or MDR solution and Dark Web monitoring that checks for activity, including the sale of credentials or mention of your organization's name. There is no cost for membership to the PSTA

.

Learn more about membership to the PSTA 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.

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.

Standalone ASTRO 25

Solution Overview

Motorola Solutions, Inc. (Motorola) is pleased to present the proposed cybersecurity Managed Detection and Response (MDR) services for City of Greensboro (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:

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

Site Information

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

Table 1-1: Site Information

Site / Location	Quantity
Core Site	1
DSR	0
Control Room CEN	0
Co-located CEN	1
Remote CEN	0
Network Management Clients	6

Site / Location	Quantity
Dispatch Consoles	0
AIS	0
CEN Endpoints	20

Services Included

The ActiveEye[SM] service modules included in our proposal are shown in the tables 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
Log Collection / Analytics	Online Storage Period: 30 Day Storage Extended Log Storage Length: 12 Months	RNI CEN
Network Detection	Up to 1 Gbps per sensor port	RNI CEN
External Vulnerability Scanning	Features in Service Modules Section	RNI CEN
Endpoint Detection and Response (EDR)	Online Storage Period: 30 Day Storage	RNI CEN

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; deploying cybersecurity countermeasures for incident containment, requesting additional information from the Customer, continuing to monitor the event for further development, or informing the Customer to enact the Customer's documented Incident Response plan.

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

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

Managed Detection and Response Elements

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

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 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.

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.

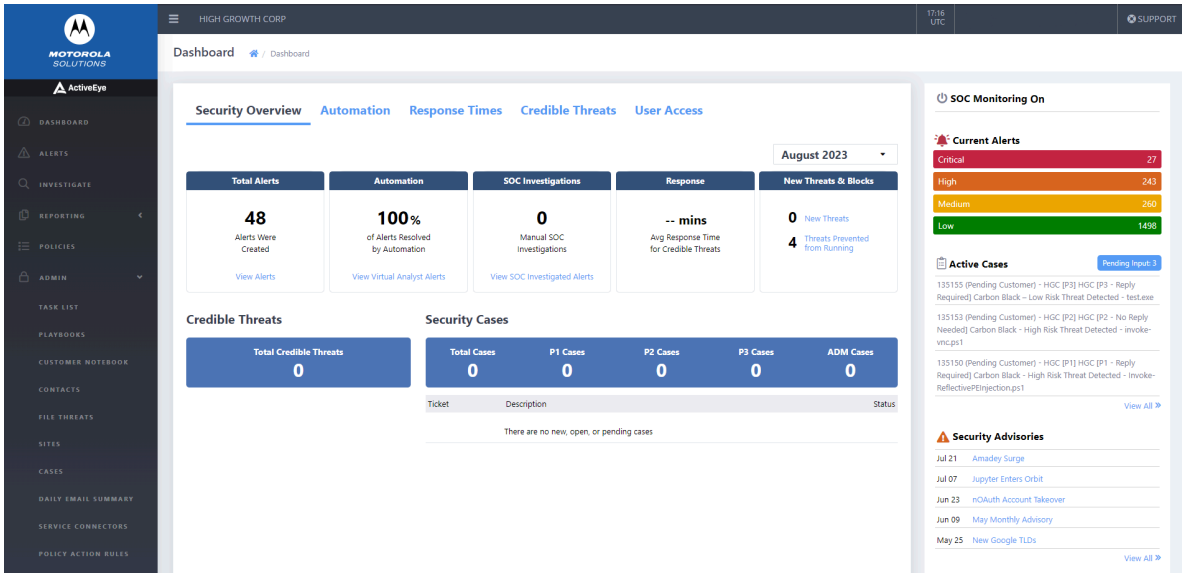

Figure 1-1: ActiveEye^{SM} Portal

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.

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.

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.

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.

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.

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.

External Vulnerability Scanning

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

Endpoint Detection and Response

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

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

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

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.

Statement of Work Standalone ASTRO 25

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 Customer Name (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.

Description of Service

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.

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

Phase 3: System Buildout and Deployment

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

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

Phase 4: Monitoring "Turn Up"

Motorola will verify 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^{SM} 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.

General Responsibilities

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.
- Integrate EDR agents as per the “Deployment Timeline and Milestones” section in all network segments where endpoint detection and response is in scope
- Note that network segments with insufficient connectivity to support endpoint detection and response will be considered out of scope for endpoint detection and response
- Motorola Solutions will perform the installation of endpoint detection and response agents in the RNI-DMZ CEN(s) and Control Room CEN(s) for all - Motorola Solutions managed devices that support endpoint detection and response agents.
- Motorola Solutions will support the customer with installing endpoint detection and response agents in the RNI-DMZ CEN(s) and Control Room CEN(s) for any device that supports endpoint detection and response agents and is not Motorola Solutions managed. Due to the fact that Motorola Solutions does not typically manage the devices and network connectivity for endpoints in the Control Room CEN, it is ultimately the customer’s responsibility to perform this installation.
- Assist the Customer with the installation of log forwarding agents on systems that are not managed by Motorola Solutions. Note, Motorola Solutions will perform installation on all endpoints that are managed by Motorola Solutions.
- 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 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 that applicable CEN systems have been configured to forward Syslog events to the AERSS.
- Provide the Customer with access to the ActiveEyeSM platform enabling Customer access to security event and incident details.

Customer Responsibilities

- The ASTRO 25 MDR service requires a connection from the Customer’s ASTRO 25 network and applicable CEN systems to the Internet. Establish connectivity with sufficient bandwidth before 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 an ASTRO site link will be leveraged for endpoint detection and response communications, that site link must support a minimum of 2 Mbps of bandwidth.
- 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.

Service Modules

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

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 ActiveEyeSM as defined.
- If applicable, configure any Customer managed devices in the CEN to forward data to ActiveEyeSM.

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

Network Detection

The AERSS deploys a Network Intrusion Detection System (NIDS), constantly monitoring traffic passing across, into, or out of 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 ActiveEyeSM as defined.
- For Customer's owned CEN infrastructure, configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a port(s) on a switch) network traffic to the ActiveEyeSM sensor.
- Initiate recommended response actions when active attacks are detected.

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

External Vulnerability Scanning

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

The initial scan results will be discussed with the Customer during service onboarding. Subsequent scans will be reviewed by a cybersecurity analyst. If any new findings of interest surface, 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 ActiveEyeSM 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.

Endpoint Detection and Response

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

Motorola Responsibilities

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

Customer Responsibilities

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

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

Security Operations Center Monitoring and Support

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.

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.

Technical Support

ActiveEye[SM] Security Management Technical Support provides the Customer with a toll-free telephone number and email address for ActiveEye[SM] 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 ActiveEyeSM.

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[SM] Security Management platform and does not include use or implementation of third-party components.

Incident Response

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

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

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

Motorola Responsibilities

- Upon the identification of an IoC, notify the Customer's documented contact and initiate the escalation plan.
- Take documented, Customer approved actions in an attempt to contain an IoC to the extent enabled via Motorola managed technology. Communicate to the Customer any additional potential containment actions and incident response resources that can be taken across the Customer’s managed IT infrastructure.
- Perform investigation using the ActiveEyeSM 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.

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.

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.

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.

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.

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.

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.

ActiveEye^{SM} 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^{SM} Platform services. Service availability is subject to limited scheduled downtime for servicing and upgrades, as well

as unscheduled and unanticipated downtime resulting from circumstances or events outside of Motorola's reasonable control, such as disruptions of, or damage, to the Customer's or a third-party's information or communications systems or equipment, telecommunication circuit availability/performance between Customer sites, any on-premises core and/or between on-premises equipment and the ActiveEye^{SM} Platform.

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.

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.

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

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

Customer and Third Party Information

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.

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.

Pricing Summary

Pricing Summary	
Cybersecurity - MDR Pricing Per Year	
Year 1	$118,973.46
Year 2	$42,300.40
Year 3	$43,992.42
Year 4	$45,752.12
Year 5	$47,582.20
ASTRO MDR Subtotal	**$298,600.60**

Quote is valid for 90 days from the date of this proposal.

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:	

1.1 Payment Schedule & Terms

Period of Performance

The contract will cover the initial period outlined in the pricing, starting 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.

Professional Services, if included, will begin upon a mutually agreed upon date after contract execution and are contingent upon completion of any related equipment/installation configuration. The project will follow the general schedule shown. The period of performance shall be completed 12 months after kick-off, or may be extended if agreed to in writing by both parties.

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 above.

Thereafter, if applicable, 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. If the optional pricing is selected, Customer-generated Purchase Order will include it.

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.

1.2 Notice to Proceed

By signing this proposal, this Notice to Proceed (NTP) serves as authorization for Motorola Solutions to place an order and invoice for the cybersecurity equipment and services as referenced herein for the purchase price listed above, subject to the terms and conditions of the next section.

Title and Risk of Loss to Equipment shall pass to Customer upon shipment from Motorola. Unless otherwise agreed by the parties in writing, shipment will be made in a manner determined by Motorola. This NTP will take precedence with respect to conflicting or ambiguous terms.

Customer affirms funding has been encumbered for this order in accordance with applicable law and will pay all proper invoices as received from Motorola solely against this Agreement.

Contractual Documentation

PRODUCTS AND SERVICES AGREEMENT

This Products and Services Agreement (this "**Agreement**") is entered into between **Motorola Solutions Inc.,** ("**Seller**" or "**Motorola**") and the entity set forth in section I(b) ("**Customer**") as of the date last signed below ("Effective Date"). Seller and Customer will each be referred to herein as a "**Party**" and collectively as the "**Parties**".

Seller and Customer Information

	Seller	Motorola Solutions, Inc.
	Customer	Name:_____ Address:_____ Contact:_____

Transaction Details

	Proposal	Proposal No.:_____ Date: _____ Motorola will provide Customer with the products and services set forth in the proposal dated above (the "Proposal"), a copy of which is attached hereto and incorporated herein.
	Pricing	Pricing for products and services being purchased by Customer is set forth in the Proposal.
	Terms and Conditions	The Parties acknowledge and agree that the terms of the Motorola Customer Agreement ("MCA"), including all applicable addenda, are incorporated herein and shall apply to the products and services provided to Customer as set forth in the Proposal. A copy of the MCA is available upon request.

Entire Agreement

This Agreement, including the Proposal and any terms and conditions referenced herein, constitutes the entire agreement of the Parties regarding the subject matter of the Agreement 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 shall 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, including by email. An electronic signature, or a facsimile copy or computer image, such as a PDF or tiff image, of a signature, shall be treated as and shall have the same effect as an original signature. In addition, an electronic signature, a true and correct facsimile copy or computer image of this Agreement shall be treated as and shall 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 or purchase order, acknowledgment or other form will not be considered an amendment or modification of this Agreement, even if a representative of each Party signs that document, and the terms of this Agreement will take precedence.

CUSTOMER:	MOTOROLA SOLUTIONS INC.
By:_____	By:_____
Print Name:_____	Print Name:_____
Title:_____	Title:_____
Date:_____	Date:_____

Attachment J

Insert PCTEL contract

Quotation

In accordance with your inquiry, PCTEL is pleased to quote the price on the requested items as follows:

Quote Number:	GRNSBRO+GLFDCO_LCS (25-28) R3	Quote Date:	12-08-24
Customer:	City of Greensboro-NC Guilford County	PCTEL:	Jason Chambers – Public Safety Sales Director
User name:	Lewis Cheatham	Tel:	850-803-8971
User tel	(336) 373-7714		
User email:	lewis.cheatham@greensboro-nc.gov	Email:	jason.chambers@pctel.com

City of Greensboro & Guilford County Life-Cycle Services (July 2025 thru June 2028)
In this proposal:

1) 3-Years Life Cycle Service Coverage for six (6) SeeHawk Monitor RTUs
    a. Three (3) RTUs for Guilford County
    b. Three (3) RTUs for City of Greensboro
2) 3-Years SeeHawk Reports SW Maintenance
3) 3-Years SeeHawk Touch/Central SW Maintenance

****NOTE****

The above outline synchronizes all licenses to come due for renewal during the same month each year. In order to qualify for the "Valued Customer Discount", the client must issue a Purchase Order (PO#) to PCTEL, Inc by May 31st, 2025.

Part Numbers & Pricing provided in the Pricing Table on Next Page:

LIFE-CYCLE SERVICES JUL 2025 thru JUN 2026						
Part Number	***Description***	***QTY***	***Market Price (Per Unit)***	***Market Price (Total)***	***Valued Customer Discount***	***Total (With Discount)***
SeeHawk Monitor - Life Cycle Services (JUL 2025 -JUN 2026)						
OPS177	SeeHawk Monitor Maintenance, Calibration, Warranty Extension per RTU (Guilford County)	6	$4,485.00	$26,910.00	7%	$25,026.30
	Additional Years - Firmware/Software Updates/ Technical Support/Extended Warranty/ RTU Calibration FOR ESN's: 42212009; 42302001; 42302009; 42212001; 42212002; 42212003					
Part Number	***Description***	***QTY***	***Market Price (Per Unit)***	***Market Price (Total)***	***Valued Customer Discount***	***Total (With Discount)***
P25 Field Test Kit - Life Cycle Services						
OPS178-F	SeeHawk Touch/Central Annual Maintenance SW Support for Permanent or Transferable License	1	$1,400.00	$1,400.00	7%	$1,302.00
OPS176-C	SeeHawk Collect Playback with Maps and Reports Annual Maintenance for Cloud License	1	$943.00	$943.00	7%	$876.99
	TOTAL (excluding taxes and shipping)			$29,253.00		**$27,205.29**

LIFE-CYCLE SERVICES JUL 2026 thru JUN 2027						
Part Number	***Description***	***QTY***	***Market Price (Per Unit)***	***Market Price (Total)***	***Valued Customer Discount***	***Total (With Discount)***
SeeHawk Monitor - Life Cycle Services (JUL 2026 -JUN 2027)						
OPS177	SeeHawk Monitor Maintenance, Calibration, Warranty Extension per RTU (Guilford County)	6	$4,485.00	$26,910.00	7%	$25,026.30
	Additional Years - Firmware/Software Updates/ Technical Support/Extended Warranty/ RTU Calibration FOR ESN's: 42212009; 42302001; 42302009; 42212001; 42212002; 42212003					
Part Number	***Description***	***QTY***	***Market Price (Per Unit)***	***Market Price (Total)***	***Valued Customer Discount***	***Total (With Discount)***
P25 Field Test Kit - Life Cycle Services						
OPS178-F	SeeHawk Touch/Central Annual Maintenance SW Support for Permanent or Transferable License	1	$1,400.00	$1,400.00	7%	$1,302.00
OPS176-C	SeeHawk Collect Playback with Maps and Reports Annual Maintenance for Cloud License	1	$943.00	$943.00	7%	$876.99
	TOTAL (excluding taxes and shipping)			$29,253.00		**$27,205.29**

LIFE-CYCLE SERVICES JUL 2027 thru JUN 2028						
Part Number	***Description***	***QTY***	***Market Price (Per Unit)***	***Market Price (Total)***	***Valued Customer Discount***	***Total (With Discount)***
SeeHawk Monitor - Life Cycle Services (JUL 2026 -JUN 2027)						
OPS177	SeeHawk Monitor Maintenance, Calibration, Warranty Extension per RTU (Guilford County)	6	$4,485.00	$26,910.00	7%	$25,026.30
	Additional Years - Firmware/Software Updates/ Technical Support/Extended Warranty/ RTU Calibration FOR ESN's: 42212009; 42302001; 42302009; 42212001; 42212002; 42212003					
Part Number	***Description***	***QTY***	***Market Price (Per Unit)***	***Market Price (Total)***	***Valued Customer Discount***	***Total (With Discount)***
P25 Field Test Kit - Life Cycle Services						
OPS178-F	SeeHawk Touch/Central Annual Maintenance SW Support for Permanent or Transferable License	1	$1,400.00	$1,400.00	7%	$1,302.00
OPS176-C	SeeHawk Collect Playback with Maps and Reports Annual Maintenance for Cloud License	1	$943.00	$943.00	7%	$876.99
	TOTAL (excluding taxes and shipping)			$29,253.00		**$27,205.29**

1. All purchase orders are subject to acceptance by confirmation in writing by PCTEL's authorized officer.
2. This Quotation is valid for thirty (30) days from Quote Date unless otherwise indicated.
3. Delivery of all Products ordered by Buyer shall be made, and title and risk of loss shall pass to Buyer in accordance with, EXW (Ex-Works) PCTEL's point of shipment.

The additional Terms and Conditions of Sale that follow are part of this Quotation.

General Terms and Conditions of Sale

SPECIAL NOTICE: As a result of the ruling by the United States Department of Commerce, Bureau of Industry and Security (BIS) on May 16, 2019 adding Huawei Technologies Co., Ltd. and 68 of its subsidiaries and affiliates ("Huawei") to the Entity List maintained under the Export Administration Regulations, many of PCTEL's test and measurement products (including its scanning receivers) cannot be sold directly or indirectly to Huawei unless authorized by a separate license issued by the Commerce Department or unless eligible for a Temporary General License. Please see the published notification from BIS **(Docket No. 190513445-9445-01).**

1. **Purchase Orders**. Any purchase order ("Purchase Order") submitted by Buyer and accepted by PCTEL, Inc. ("PCTEL"), shall be subject to these General Terms and Conditions of Sale (these "General Terms"). PCTEL objects to any terms proposed by Buyer in a purchase order or otherwise, which add to, vary from or conflict with these General Terms. Any such proposed terms shall not operate as a rejection of these General Terms, but are deemed a material alteration, and these General Terms shall be deemed accepted by Buyer without said additional or different terms. "**Buyer**" as used in these General Terms shall refer to the purchaser, whether an individual, a partnership, a company or any other type of entity or organization. "**Product**"as used in these General Terms shall mean devices, receivers, transmitters, systems, copies of Software, related materials or documentation, and related parts and components sold or licensed to Buyer by PCTEL.

2. **Software**. "**Software**" shall mean the software, in object code form, or software programs incorporated in or provided directly or indirectly by PCTEL to be used in connection with the Products, including any corrections, updates, upgrades, enhancements, new releases, new versions, patches and other modifications made thereto. PCTEL expressly reserves all title and ownership in and to the Software (and all copies thereof), in any form. Title to the Software shall not pass to Buyer at any time. PCTEL will grant a personal, non-exclusive, non-transferable right and license to Buyer to install and/or use the Software solely as embedded in or in conjunction with the Products. Buyer will be prohibited from copying, distributing, modifying, adapting, reverse engineering, disassembling, or preparing derivative works of the Software.

3. **Price and Payment**. All invoices shall be paid in United States Dollars. Late charges will be imposed on past due accounts at an interest rate which shall be the lower of the maximum legal rate at the time the purchase order is accepted or 1.5% per month. PCTEL may request a deposit or progress payments in conjunction with custom Products or large Product orders. In all other cases, payment is due immediately prior to shipment of the Products to Buyer. The foregoing notwithstanding, if Buyer desires to purchase the Products on thirty (30) day credit terms, Buyer may complete the PCTEL Credit Application form (the "**Application**") and submit it to PCTEL for consideration. If Buyer's Application is approved by PCTEL in its sole discretion, Buyer may pay the invoiced amount of the Products within thirty (30) days of the date of the invoice. If Buyer is located in the United States, Buyer may pay the invoiced amount of the Products as follows: (i) by Automated Clearing House (ACH), (ii) by wire transfer of immediately available funds to the account specified by PCTEL, or (iii) if Buyer's Application is approved, by corporate check in accordance with the instructions provided by PCTEL. If Buyer is located in a country other than the United States, payment must be made by wire transfer of immediately available funds to the account specified by PCTEL or by such other means of payment approved in writing by PCTEL. Product prices are exclusive of any federal, state, or local excise, sales, use, value added, or other taxes, customs, duties, or similar tariffs and fees, which shall be the responsibility of Buyer. Unless otherwise stated, prices do not include installation instruction or other special documentation costs, or costs for special packaging materials, each of which will be quoted separately based upon Buyer's requirements.

4. **Delivery**. Delivery of all Products ordered by Buyer shall be made, and title and risk of loss shall pass to Buyer in accordance with, EXW (Ex-Works) PCTEL's point of shipment. Buyer shall be solely responsible for the expenses associated with shipping, including shipping for return and redelivery of the Products to be upgraded. Warranty shipping is covered under 6(C). ICC Incoterms 2020 shall apply to international shipments, except insofar as the Incoterms may be inconsistent with the express provisions of these General Terms. PCTEL shall not be liable for failure to perform any obligation under any purchase order or any loss, damage, or delay due directly or indirectly to causes beyond the control and without the fault or negligence of PCTEL, including, without limitation: (i) acts of God or unusually severe weather conditions, including earthquake, storm, fire, or flood; (ii) acts of the public enemy, war, hostility, or invasion; (iii) civil disturbances, riots, or insurrections; (iv) public health issues, including epidemics and pandemics; (v) any accident, explosion, sabotage, or similar disruption; (vi) any labor difficulty (whether general, local, or confined to a particular group of employees, including but not limited to strikes, lockouts, work stoppages, or refusal to cross a picket line); and (vii) any transportation difficulty, wreck, accident, or traffic delay.

5. **Cancellation.** No cancellation or return of custom or special Products is permitted. PCTEL may, in its sole discretion, approve in writing the cancellation or return of certain standard Products, subject to a restocking fee.

6. **Inspection; Warranty.**

A. Inspection. Buyer shall promptly inspect the shipped Products for accuracy and completeness, and shall notify PCTEL of any deficiency within ten (10) days of receipt. In the event Buyer fails to give written notice to PCTEL of any deficiency in the foregoing (specifying the basis of the claim in detail) within such time period, Buyer waives any claim related to such deficiency. In the event that PCTEL receives written notice of such a deficiency, PCTEL will promptly correct any short or incorrect shipment at its own expense and will repair or replace defective Products in accordance with the terms of paragraph 6(B).

B. General Warranty. PCTEL warrants that the Products furnished hereunder shall be free from defects in material and workmanship under normal use and operation for the following periods of time commencing with the date of shipment by PCTEL:

Warranty Period	Description of Products
5 years	MX*flex*®, and IB*flex*® scanning receivers[1]
3 years	G*flex*™ scanning receivers
2 years	HB*flex*™ and IB*flex*® Lite scanning receivers[2] SeeHawk Monitor hardware
1 year	SeeGull® CW Transmitters SeeWave® interference locating system hardware TX2440 mmWave Transmitter PCTEL battery products
6 months	Antennas – OP318 and OP319 Amp mmWave Ant,24-40GHz
1 Year or Pass-Through Warranty Offered by applicable Third Party Manufacturer (whichever is greater)	CW Transmitter 23.5 MHz – 6.0 GHz (OP712) [3] Any other Products

[1] Except in situations involving an upgrade from:

- a SeeGull® MX Scanning Receiver to an a MX*flex*® scanning receiver, or
- an IB*flex*® model 0890x Scanning Receiver to an IB*flex*® model 0890x-E scanning receiver, or
- a SeeGull® EX or EX*flex*® scanning receiver to an IB*flex*® scanning receiver,

in which cases the warranty period shall be the longer of (i) 2 years or (ii) the remaining warranty period on the scanning receiver being upgraded.

[2] Except in situations involving an upgrade from an IB*flex*® or IB*flex*® Lite scanning receiver to an HB*flex*™ scanning receiver, in which case the warranty period shall be the shorter of (i) 2 years or (ii) the remaining warranty period on the scanning receiver being upgraded.

[3] The 2 year pass-through warranty, as well as warranty service, are provided by AudioVideo BrandBuilder Corporation.

PCTEL does not provide a warranty on the SeeWave®, SeeHawk® Collect, SeeHawk® Touch, SeeHawk™ Central Software applications or any other Software. Software is licensed and not sold. Each license for SeeWave, SeeHawk Collect, and SeeHawk Touch includes a subscription for support and maintenance for an initial period. PCTEL may offer renewals or extensions of subscriptions for support and maintenance. SeeHawk Central is provided as SAAS on a subscription basis requiring maintenance of a subscription in order to continue using the Software/system and receiving support.

PCTEL's sole and exclusive obligation under the foregoing warranty is, at its option, to repair or replace any defective Product that fails during the warranty period. The expense of removal and reinstallation of any item is not included in this warranty. THE

FOREGOING WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE WITH RESPECT TO THE PRODUCTS. Repair or replacement in the manner provided herein shall be the sole and exclusive remedy of the Buyer for breach of warranty and shall constitute fulfillment of all liabilities of PCTEL with respect to the quality and performance of the Products.

The foregoing warranty shall apply only if: (a) the Product has been properly installed and used at all times in accordance, in all material respects, with the applicable Product documentation; (b) no modification, alteration or addition has been made to the Product by persons other than PCTEL or PCTEL's authorized representatives or otherwise approved by PCTEL in writing; and (c) the Product has not been subjected to abuse, misuse, neglect or unusual physical, electrical or electromagnetic stress, or some other type of accident. PCTEL DOES NOT WARRANT THAT THE OPERATION OF THE PRODUCTS IS ERROR-FREE OR THAT OPERATION WILL BE UNINTERRUPTED. IN NO EVENT SHALL PCTEL BE LIABLE FOR: (i) ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES TO THE BUYER OR ANY THIRD PARTY, WHETHER THE CLAIM IS BASED UPON CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, (ii) THE BUYER'S SELECTION OF PRODUCTS FOR THE BUYER'S APPLICATION, AND/OR (iii) FAILURE OF PRODUCTS TO MEET GOVERNMENT OR REGULATORY REQUIREMENTS. PCTEL'S MAXIMUM AGGREGATE LIABILITY TO THE BUYER SHALL BE LIMITED TO THE TOTAL AMOUNT PAID BY THE BUYER TO PCTEL FOR THE SPECIFIC PRODUCTS FROM WHICH LIABILITY ARISES. THE FOREGOING EXCLUSIONS AND LIMITATIONS OF LIABILITY AND DAMAGES SHALL NOT APPLY TO DAMAGES FOR PERSONAL INJURY.

C. Warranty Procedures. In the event of a warranty claim, the Buyer must contact PCTEL to arrange for Product return. No Product will be accepted for replacement or repair without first obtaining a Return Material Authorization (RMA) number from the PCTEL website at www.pctel.com/support/product-returns-rma, or by contacting PCTEL Customer Service by telephone at 1-240-460-8833 or by email at support.rfsg@pctel.com. PCTEL reserves the right to inspect all defective Products. Products returned without an RMA number will not be processed and will be returned to the Buyer freight collect. The warranty period of any repaired or replaced Product shall not extend beyond the original term of the warranty on the Product repaired or replaced. Product to be repaired or replaced under warranty is to be returned, freight prepaid, to the following address with the assigned RMA number displayed on the box:

PCTEL, Inc.
Attn: RMA Coordinator
22600 Gateway Center Drive, Suite 100
Clarksburg, MD 20871 USA

7. **Confidential and Proprietary Information**. Any Software, information, data, drawings, pricing, manuals, and other documents (collectively, "Documents") transmitted by PCTEL to Buyer shall be deemed PCTEL Confidential Proprietary Information, shall remain PCTEL's property, shall be kept confidential by Buyer and its employees, agents, officers and directors, and shall be promptly returned to PCTEL at PCTEL's request. Buyer acknowledges that the Software contains valuable proprietary information and trade secrets of PCTEL and that unauthorized or improper use of Software may result in irreparable harm to PCTEL for which monetary damages would be inadequate and for which PCTEL will be entitled to immediate injunctive relief. Buyer shall not disclose, without PCTEL's written permission, any Documents to any other person (other than to Buyer's employees having a need to know, and its attorneys, accountants, and other professional advisors as reasonably necessary, or as required by law or pursuant to a court decree). The obligations of this Section shall survive cancellation, termination, or completion of Buyer's Purchase Order.

8. **Indemnification.**

A. PCTEL Indemnification Obligations. PCTEL shall defend Buyer in any lawsuit and pay (i) any damages finally awarded, or (ii) any settlement of such lawsuit as provided below (in either case, including but not limited to reasonable attorneys' fees) resulting from any third party claim alleging that the Product, when properly used as contemplated herein, directly infringes any copyright, trade secret or U.S. patent of any third party. THE FOREGOING STATES THE ENTIRE LIABILITY OF PCTEL, AND THE SOLE REMEDY OF BUYER, WITH RESPECT TO ANY ACTUAL OR ALLEGED CLAIM OF INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS. In the event of an infringement claim against Buyer as described above or in the event PCTEL believes such a claim is likely, PCTEL shall have

the option, at its expense, to (i) modify the Product so that it is non-infringing; or (ii) obtain for Buyer a right to continue using the Product. If it is not commercially reasonable to perform either of the above options, then PCTEL may terminate Buyer's right to obtain, resell and use the Product.

B. Exclusions. Notwithstanding the foregoing, PCTEL shall have no obligation to indemnify Buyer pursuant to paragraph 8(A) above with respect to any infringement or alleged infringement resulting from, or relating to, (i) any modification to the Product made by any person other than PCTEL or its authorized representative, (ii) any modification made to the Product by PCTEL at Buyer's specific direction, (iii) any unauthorized use of the Product by Buyer, its customer, or any other third party, (iv) any use of the Product in combination with other products, devices, hardware, software, or data, where, but for such combination, no infringement involving the Product would have occurred, or (v) the CW Transmitter 35 MHz – 4.4 GHz (OP711).

C. Buyer Indemnification Obligations. Buyer shall defend PCTEL and its officers, directors and employees in any lawsuit and pay (i) any damages finally awarded, or (ii) any settlement of such lawsuit (in either case, including but not limited to reasonable attorneys' fees) resulting from any third party claim against PCTEL arising out of (a) any representations or warranties regarding the capabilities, performance, functional characteristics or compatibilities of the Product beyond or inconsistent with the description set forth in the documentation provided by PCTEL; (b) the sale, distribution or use of a Product in connection with any other product, device, hardware, software, or data offered by Buyer, except to the extent that any such claim arises out of any infringement claims covered by paragraph 8(A) after application of the exclusions in paragraph 8(B) above; (c) any breach by Buyer of its representations and warranties hereunder; or (d) any claim (including a claim for personal injury or property damage) asserting that any Product, when bundled with any other product, device, hardware, software or data or sold as a system using other such items, is defective or unreasonably dangerous or fails to comply with a warranty made by Buyer. THE FOREGOING PROVISIONS OF THIS PARAGRAPH (C) STATE THE ENTIRE LIABILITY OF BUYER, AND THE SOLE REMEDY OF PCTEL, WITH RESPECT TO ANY ACTUAL OR ALLEGED CLAIMS AS DESCRIBED IN SUBSECTIONS (a) THROUGH (d).

D. Indemnification Procedures. If a party entitled to indemnification under this paragraph 8 (an "**Indemnified Party**") makes an indemnification request to the other party ("**Indemnifying Party**"), the Indemnified Party shall permit the other party to control the defense, disposition or settlement of the matter at its own expense; provided that the Indemnifying Party shall not, without the consent of the Indemnified Party, enter into any settlement that imposes any obligations on the Indemnified Party other than the payment of monies that are readily measurable for purposes of determining the indemnification obligations of the Indemnifying Party. The Indemnified Party shall notify the Indemnifying Party promptly of any claim for which the Indemnifying Party is responsible and shall reasonably cooperate with the Indemnifying Party to facilitate the defense of any such claim.

9. **Export Restrictions**. Buyer agrees to comply with all applicable export laws, restrictions and regulations of the United States and any other relevant jurisdiction. This includes the U.S. Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR), as well as all other laws, restrictions and regulations administered by the U.S. Department of Commerce, U.S. Department of State, U.S. Department of Defense, U.S. Department of Homeland Security, and any other relevant domestic or foreign agency or authority. Buyer agrees not to export, or allow the export or re-export, of any Products or related technical data in violation of any such laws, restrictions, or regulations. Buyer shall indemnify PCTEL for all liabilities, penalties, losses, damages, costs, or expenses (including attorneys' fees) incurred by PCTEL in connection with any violations of such laws, restrictions, and regulations.

10. **Choice of Law.** These General Terms shall be governed by and construed under the laws of the State of Illinois, excluding that body of law pertaining to conflict of laws. The rights and obligations of the parties shall not be governed by the provisions of the United Nations Convention on Contracts for the International Sales of Goods.

11. **Dispute Resolution**. PCTEL and Buyer will attempt to settle any claim or controversy between them (other than disputes involving intellectual property) through good faith consultation and negotiation. If the parties are unable to settle any such dispute within thirty (30) days, the parties agree to settle such dispute (other than disputes involving intellectual property) through mediation or other form of alternate dispute resolution ("ADR"). If the parties are unable to agree on the form of ADR, the matter shall be submitted to arbitration to be arbitrated by one arbitrator. The ADR or arbitration proceeding shall take place in Cook County, Illinois and be conducted in the English language. Notwithstanding the foregoing, any dispute with respect to intellectual property rights shall be submitted to the U.S. District Court for the Northern District of Illinois and not be referred to ADR or arbitration as described above.

12. **Notices.** All notices, demands, requests or other communications which may be or are required to be given, served, or sent by either party to the other party shall be in writing and shall be hand delivered or sent by courier, addressed to each party at the address shown on the relevant quotation, purchase order, confirmation, or invoice. Each party may designate by written notice a new address to which any notice, demand, request, or communication may thereafter be delivered, given, served, or sent. Documents delivered by hand shall be deemed to have been received upon delivery, and documents sent by courier shall be deemed to have been received upon receipt or at such time as delivery is refused by addressee upon presentation.

13. **Entire Agreement**. These General Terms and any documents in which they are referenced constitute the entire agreement between PCTEL and Buyer and supersede all prior understandings etween PCTEL and Buyer, and supersede all prior understandings or agreements on the subject matter.

Attachment K

Insert Cost Sheet

Infrastructure and Monitoring							
Vendor		FY26	FY27	FY28	FY26-FY28	FY29	FY30
	Motorola SUAII	$ 1,369,986.17	$ 1,369,986.17	$ 1,369,986.17	$ 4,109,958.51	$ 1,369,986.17	
	County Share (50%)	$ 684,993.09	$ 684,993.09	$ 684,993.09	$ 2,054,979.26	$ 684,993.09	
	Motorola Managed Detection and Response services	$ 118,973.46	$ 42,300.40	$ 43,992.42	$ 205,266.28	$ 45,752.12	$ 47,582.20
	County share (50%)	$ 59,486.73	$ 21,150.20	$ 21,996.21	$ 102,633.14	$ 22,876.06	$ 23,791.10
	MCM Technology LLC	$ 30,529.55	$ 31,750.73	$ 33,020.76	$ 95,301.04		
	County Share (50%)	$ 15,264.78	$ 15,875.37	$ 16,510.38	$ 47,650.52		
	Genesis	$ 21,379.78	$ 22,021.18	$ 22,681.81	$ 66,082.77		
	County Share (50%)	$ 10,689.89	$ 11,010.59	$ 11,340.91	$ 33,041.39		
	PCTEL				$ -		
	Maintenance of SeeHawks (6-100%)	$ 27,205.29	$ 27,205.29	$ 27,205.29	$ 81,615.87		
	Purchase of 3 SeeHawks (100% County)				$ -		
	Maintenance of SeeHawks (50%)	$ 13,602.65	$ 13,602.65	$ 13,602.65	$ 40,807.94		
	TOTAL	$ 1,568,074.25	$ 1,493,263.77	$ 1,496,886.45	$ 4,558,224.47		
	County Share	$ 784,037.13	$ 746,631.89	$ 748,443.23	**$ 2,279,112.24**		