

**RIDER TO ASTRO 25 MANAGED DETECTION AND RESPONSE  
PRODUCTS AND SERVICES AGREEMENT WITH MOTOROLA SOLUTIONS, INC.**

**THIS RIDER TO THE ASTRO 24 MANAGED DETECTION AND RESPONSE PRODUCTS AND SERVICES AGREEMENT WITH MOTOROLA SOLUTIONS, INC.** (hereinafter “Rider”) is made by and between the **Board of County Commissioners of Nassau County, Florida**, a political subdivision of the State of Florida (hereinafter the “County” or “Customer”), and **Motorola Solutions, Inc.**, located at **500 W Monroe Street, Ste 4400, Chicago, IL 60664-3781** (hereinafter the “Vendor”) hereinafter collectively referred to as the “Parties.”

**WITNESSETH:**

**WHEREAS**, the Parties desire to enter into a 3-year agreement for Astro 25 managed detection and response hardware, equipment and installation services as provided in that certain Products and Services Agreement between the Parties (hereinafter “Agreement”); and

**WHEREAS**, the County has determined that the good and services required are either exempt, single or sole source purchase, and as such the County has completed all necessary steps under the applicable Nassau County Purchasing Policy in regard to the sole source acquisition of the Vendor’s goods and services

**WHEREAS**, the Parties wish to establish additional standard terms and conditions to that Agreement as contained herein; and

**WHEREAS**, the Parties agree that the term and conditions hereinbelow shall be incorporated into the Agreement and in the event of any conflict between the terms and conditions of this Rider and the Agreement, the terms and conditions of this Rider shall prevail.

**NOW, THEREFORE**, for good and valuable consideration the receipt and sufficiency of which is hereby acknowledged, and intending to be legally bound, the Parties do agree to amend the Agreement as follows:

**SECTION 1. CONFLICTING PROVISIONS.**

**1.1** The Parties agree that in the event of any conflict between the terms and conditions of the Agreement and/or any exhibit or attachment to the Agreement and the terms and conditions of this Rider, the terms and conditions of this Rider shall prevail.

**SECTION 2. PAYMENT AND INVOICING.**

2.1 The County shall pay the Vendor in an amount not to exceed one hundred eighty-one thousand three hundred twenty-eight dollars and 69/100 (\$181,328.69) for the goods and/or services referenced in the Agreement over the full term of the Agreement. No payment shall be made for goods and/or services without a proper County work authorization or purchase order. The Vendor shall submit a copy of all invoices to both the Chief Innovation Officer or designee and to [invoices@nassaucountyfl.com](mailto:invoices@nassaucountyfl.com) for payment. The invoice submitted shall include the contract number referenced and shall be in sufficient detail as to item, quantity and price in order for the County to verify compliance with the specifications and conditions of Agreement. Payment shall not be made until goods and/or services have been received, inspected and accepted by the County in the quantity and/or quality ordered. Payment in advance of receipt of goods and/or services by the County cannot be made. The County shall pay the Vendor within forty-five (45) calendar days of receipt and acceptance of invoice by the Chief Innovation Officer, pursuant to and in accordance with the promulgations set forth by the State of Florida's Prompt Payment Act found at Section 218.70, Florida Statutes. The Vendor shall honor all purchase orders or work authorizations issued prior to the expiration of the term of the Agreement. The Vendor shall be responsible for all expenses incurred while providing goods and/or services under the Agreement including, but not limited to, license fees, memberships and dues; automobile and other travel expenses; meals and entertainment; insurance premiums; and all salary, expenses and other compensation paid to the Vendor's agents, if any, hired by the Vendor to complete the work under the Agreement.

**SECTION 3. E-VERIFY.**

3.1 The Vendor shall comply with Section 448.095, Florida Statutes, and use the United States Department of Homeland Security's E-Verify system ("E-Verify") to verify the employment eligibility of all persons hired by the Vendor during the term of the Agreement to work in Florida. Additionally, if the Vendor uses subcontractors to perform any portion of the work (under the Agreement), the Vendor shall include a requirement in the subcontractor's contract that the subcontractor use E-Verify to verify the employment eligibility of all persons hired by subcontractor to perform any such portion of the work. Answers to questions regarding E-Verify as well as instructions on enrollment may be found at the E-Verify website: [www.uscis.gov/e-verify](http://www.uscis.gov/e-verify).

3.2 The Vendor shall maintain records of its participation and compliance with the provisions of the E-Verify program, including participation by its subcontractors as provided above, and to make such records available to the County or other authorized entity consistent with the terms of the Vendor's enrollment in the program. This includes maintaining a copy of proof of the Vendor's and subcontractors' enrollment in the E-Verify program. If the Vendor enters into a contract with a subcontractor, the subcontractor shall provide the Vendor with an affidavit stating that the subcontractor does not employ, contract with, or subcontract with an unauthorized alien. The Vendor shall maintain a copy of such affidavit for the duration of the contract.

3.3 Compliance with the terms of the E-Verify program provision is made an express condition of the Agreement and the County may treat a failure to comply as a material breach of the Agreement. If the County terminates the Agreement pursuant to Section 448.095(2)(c), Florida Statutes, the Vendor may not be awarded a public contract for at least one (1) year after the date on which the contract was terminated and the Vendor is liable for any additional costs incurred by the County as a result of the termination of the Agreement.

**SECTION 4. GOVERNING LAW, VENUE, COMPLIANCE WITH LAWS, ATTORNEY'S FEES AND CHANGE OF LAWS.**

4.1 The Agreement shall be deemed to have been executed and entered into within the State of Florida and any dispute arising hereunder, shall be governed, interpreted and construed according to the laws of the State of Florida, the Ordinances of Nassau County, and any applicable federal statutes, rules and regulations. Any and all litigation arising under the Agreement shall be brought in Nassau County, Florida, and any trial shall be non-jury. Any mediation, pursuant to litigation, shall occur in Nassau County, Florida.

4.2 The Vendor shall secure and maintain all licenses and permits required to provide goods and/or services under the Agreement and to pay any and all applicable sales or use tax, or any other tax or assessment which shall be imposed or assessed by any and all governmental authorities, required under the Agreement.

4.3 The Vendor shall comply with all federal, state, county and municipal laws, ordinances, policies and rules including Title I of the Americans with Disabilities Act and the County's adopted Web Content Accessibility Guidelines (WCAG), version 2.1, level AA.

4.4 In the event of any legal action to enforce the terms of the Agreement each party shall bear its own attorney's fees and costs.

4.5 If there is a change in any state or federal law, regulation or rule or interpretation thereof, which affects the Agreement or the activities of either party under the Agreement, and either party reasonably believes in good faith that the change will have a substantial adverse effect on that party's rights or obligations under the Agreement, then that party may, upon written notice, require the other party to enter into good faith negotiations to renegotiate the terms of the Agreement. If the parties are unable to reach an agreement concerning the modification of the Agreement within fifteen (15) days after the date of the notice seeking renegotiation, then either party may terminate the Agreement by written notice to the other party. In such event, Vendor shall be paid its compensation for the goods and/or services provided prior to the termination date.

**SECTION 5. TAXES.**

5.1 The Vendor recognizes that the County, by virtue of its sovereignty, is not required to pay any taxes on the goods and/or services provided under the terms of the Agreement. As such, the Vendor shall refrain from including taxes in any billing. Any questions regarding this tax exemption shall be addressed to the County Manager.

**SECTION 6. FUNDING.**

6.1 The County's performance and obligation under the Agreement is contingent upon an annual appropriation by the Board of County Commissioners for subsequent fiscal years and is subject to termination based on lack of funding. Notwithstanding the above, the County will pay Vendor for all conforming services rendered, and equipment or parts provided, up to the date of termination.

**SECTION 7. PUBLIC RECORDS.**

7.1 The County is a public agency subject to Chapter 119, Florida Statutes. **IF THE VENDOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE VENDOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THE AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (904) 530-6090, RECORDS@NASSAUCOUNTYFL.COM, 96135 NASSAU PLACE, SUITE 6, YULEE, FLORIDA 32097.** Under the Agreement, to the extent that the Vendor is providing goods and/or services to the County, and pursuant to Section 119.0701, Florida Statutes, the Vendor shall:

- a. Keep and maintain public records required by the County to provide goods

and/or services.

- b. Upon request from the County's custodian of public records, provide the County with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in this chapter or as otherwise provided by law.
- c. Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the Agreement term and following completion of the Agreement if the Vendor does not transfer the records to the County.
- d. Upon completion of the Agreement, transfer, at no cost, to the County all public records in possession of the Vendor or keep and maintain public records required by the County to perform the service. If the Vendor transfers all public records to the County upon completion of the Agreement, the Vendor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Vendor keeps and maintains public records upon completion of the Agreement, the Vendor shall meet all applicable requirements for retaining public records. All records stored electronically shall be provided to the County, upon request from the County's custodian of public records, in a format that is compatible with the information technology systems of the County.

**7.2** A request to inspect or copy public records relating to the Agreement for goods and/or services shall be made directly to the County. If the County does not possess the requested records, the County shall immediately notify the Vendor of the request, and the Vendor shall provide the records to the public agency or allow the records to be inspected or copied within a reasonable time.

**7.3** If the Vendor does not comply with the County's request for records, the County shall enforce the Agreement provisions in accordance with the Agreement.

**7.4** If the Vendor fails to provide the public records to the County within a reasonable time, the Vendor may be subject to penalties under Section 119.10, Florida Statutes.

**7.5** If a civil action is filed against the Vendor to compel production of public records relating to the Agreement, the Court shall assess and award against the Vendor the reasonable costs of enforcement, including reasonable attorney fees if:

- (a) The Court determines that the Vendor unlawfully refused to comply with the public records request within a reasonable time; and
- (b) At least eight (8) business days before filing the action, the plaintiff provided written notice of the public records request, including a statement that the Vendor has not complied with the request, to the County and to the Vendor.

7.6 A notice complies with this Section if it is sent to the County's custodian of public records and to the Vendor at the Vendor's address listed on its Agreement with the County or to the Vendor's registered agent.

7.7 If the Vendor complies with a public records request within eight (8) business days after the notice is sent, the Vendor is not liable for the reasonable costs of enforcement.

7.8 In reference to any public records requested under the Agreement, the Vendor shall identify and mark specifically any information which Vendor considers CONFIDENTIAL and/or proprietary, inclusive of trade secrets as defined in Section 812.081, Florida Statutes, and which the Vendor believes to be exempt from disclosure, citing specifically the applicable exempting law and including a brief written explanation as to why the cited Statute is applicable to the information claimed as confidential and/or proprietary information. All materials shall be segregated and clearly identified as "EXEMPT FROM PUBLIC DISCLOSURE."

7.9 In conjunction with the confidential and/or proprietary information designation, the Vendor acknowledges and agrees that after notice from County, the Vendor shall respond to a notice from the County immediately, but no later than 10 calendar days from the date of notification or the Vendor shall be deemed to have waived and consented to the release of the confidential and/or proprietary designated materials.

**7.10 INTENTIONALLY DELETED.**

**SECTION 8. PUBLIC ENTITY CRIMES.**

8.1 In accordance with Section 287.133, Florida Statutes, the Vendor certifies that it, its affiliates, suppliers, subcontractors and consultants who will perform hereunder, have not been placed on the convicted vendor list maintained by the State of Florida Department of Management Services within the thirty-six (36) months immediately preceding the date of the Agreement.

**SECTION 9. INSURANCE.**

9.1 The Vendor shall provide and maintain at all times during the term of this Agreement, without cost or expense to the County, such commercial (occurrence form) or comprehensive

general liability, workers compensation, professional liability, and other insurance policies as detailed in Exhibit "A". .

**9.2** The Vendor shall provide to the County a Certificate of Insurance for all policies of insurance and renewals thereof in an Acord form acceptable to the County. Said certificates shall provide that the Nassau County Board of County Commissioners is included as an additional insured on the Commercial General Liability and Automobile Liability policies, and that the County shall be notified in writing of cancellation on the Commercial General Liability, Automobile Liability, and Workers Compensation policies at least thirty (30) days prior to the effective date of said action.. All insurance policies shall be issued by responsible companies who are reasonably acceptable to the County and licensed and authorized under the laws of the State of Florida.

#### **SECTION 10. TAXES, LIENS, LICENSES AND PERMITS.**

**10.1** The Vendor recognizes that the County, by virtue of its sovereignty, is not required to pay any taxes on the goods and/or services provided under the terms of this Agreement. As such, the Vendor shall refrain from including taxes in any billing. The Vendor is placed on notice that this exemption generally does not apply to nongovernmental entities, contractors, or subcontractors. Any questions regarding this tax exemption shall be addressed to the County Manager.

**10.2** The Vendor shall secure and maintain all licenses and permits required to provide goods and/or services under this Agreement and to pay any and all applicable sales or use tax, or any other tax or assessment which shall be imposed or assessed by any and all governmental authorities, required under this Agreement, and to meet all federal, state, county and municipal laws, ordinances, policies and rules.

**10.3** The Vendor acknowledges that property being improved that is titled to the County, shall not be subject to a lien of any kind for any reason. The Vendor shall include notice of such exemptions in any subcontracts and purchase orders issued under this Agreement.

#### **SECTION 11. INDEMNIFICATION.**

**11.1** Any indemnification by the County in the Agreement or any sub agreement, or exhibit thereunder is hereby limited to the limits as set forth in Section 768.28, Florida Statutes.

#### **SECTION 12. HUMAN TRAFFICKING AFFIDAVIT.**

**12.1** In accordance with Section 787.06, Florida Statutes, the Vendor shall provide the County an affidavit, on a form approved by the County, signed by an officer or a representative of

CM3828

the Vendor under penalty of perjury attesting that the Vendor does not use coercion for labor or services as defined in Section 787.06, Florida Statutes.

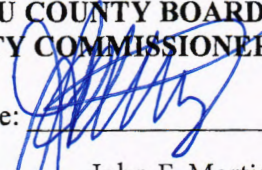
[The remainder of this page left intentionally blank. Signatures follow.]



IN WITNESS WHEREOF, the Parties have caused this Rider to be executed by its duly authorized representatives, effective as of the last date below.

**THE COUNTY:**

**NASSAU COUNTY BOARD OF COUNTY COMMISSIONERS**

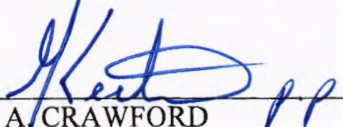
Signature:  \_\_\_\_\_

Print Name: John F. Martin, MBA

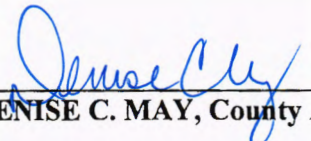
Title: Chairman

Date: 12/18/2024

**Attest as to the authenticity of the Chair's signature:**

  
\_\_\_\_\_  
JOHN A. CRAWFORD  
Its: Ex-Officio Clerk

**REVIEWED FOR LEGAL FORM AND CONTENT:**

  
\_\_\_\_\_  
DENISE C. MAY, County Attorney

**VENDOR:**

**MOTOROLA SOLUTIONS, INC.**

Signature: Daniel Sanchez

Print Name: Daniel Sanchez

Title: FL Territory VP

Date: 12/3/2024



**MOTOROLA SOLUTIONS**

**Firm Fixed Price Proposal**

**Nassau County Board of Commissioners**

# **ASTRO 25 Managed Detection and Response**

**24-181900 / Cybersecurity Services**

**October 8, 2024**

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

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

# Table of Contents

## Section 1

**Executive Summary ..... 1-1**

## Section 2

**Solution Description – ASTRO MDR ..... 2-1**  
    **2.1 Solution Overview ..... 2-1**  
    **2.2 Service Description ..... 2-2**

## Section 3

**Statement of Work – ASTRO MDR ..... 3-1**  
    **3.1 Overview ..... 3-1**  
    **3.2 Description of Service ..... 3-1**  
    **3.3 Security Operations Center Monitoring and Support ..... 3-6**

## Section 4

**Limitations and Clarifications ..... 4-1**

## Section 5

**Proposal Pricing ..... 5-1**  
    **5.1 Pricing Summary ..... 5-1**  
    **5.2 Payment Schedule & Terms ..... 5-1**  
    **5.3 Invoicing and Shipping Addresses ..... 5-2**

## Section 6

**Contractual Documentation ..... 6-1**



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

October 8, 2024

Derrick Lindsay  
CIO Nassau County BOC  
96135 Nassau Place  
Yulee, FL 32097

RE: ASTRO® Managed Detection and Response

Dear Mr. Lindsay,

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

- Providing a market leading MDR solution for Nassau County's ASTRO® network with Motorola's SOAR platform, known as ActiveEye
- Providing geographically redundant Security Operations Centers (SOC) operating 24 hours a day, 7 days per week, 365 days per year
- Notifying Nassau County Board of Commissioners of active threats and the activities used to detect/investigate possible threats through threat hunting services

We are confident that Motorola can provide a best in class premier offering of MDR and risk mitigation services to Nassau County Board of Commissioners. Motorola Solutions' proposal is conditioned upon Nassau County Board of Commissioners acceptance of the terms and conditions included with this proposal, or a mutually negotiated version thereof. This proposal shall remain valid until December 29, 2024. Any questions Nassau County Board of Commissioners has regarding this proposal can be directed to Bryce Sheffield, Cybersecurity Account Manager at 407-529-4253 or by email at [bryce.sheffield@motorolasolutions.com](mailto:bryce.sheffield@motorolasolutions.com).

Our goal is to provide you with the best products and services available in the industry to address your ongoing Cybersecurity needs. We thank you for the opportunity to provide this proposal for Managed Detection and Response for Nassau County Board of Commissioners, and we hope to strengthen our relationship by implementing this project.

Sincerely,

Mike Allen

Area Sales Manager, Cybersecurity – North America

MOTOROLA SOLUTIONS, INC.

## Section 1

# Executive Summary

Motorola is pleased to build upon our years of ongoing support to Nassau County Board of Commissioners 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.

## Cybersecurity Advisory Services

Motorola's Cybersecurity Advisory Services provides recommendations for our customers to leverage processes and systems to achieve a lower risk profile and increased cyber resilience. Our services deliver this through assessments utilizing the industry-standard cybersecurity frameworks, vulnerability scanning, and system configuration reviews.

Cybersecurity Advisory Services recommendations are in alignment with the following control sets:

- Criminal Justice Information Services (CJIS) Security Policy
- National Institute of Standards and Technology (NIST) SP800-53r5
- Center for Internet Security (CIS) Common Security Controls (CSC)
- Health Insurance Portability and Accountability Act (HIPAA)
- International Standards Organization (ISO) 27001

## The ActiveEye<sup>SM</sup> Platform

In 2020, Motorola acquired Delta Risk, a leading Managed Security Services Provider (MSSP). The acquisition now allows Motorola to extend the ActiveEye<sup>SM</sup> 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<sup>SM</sup> 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<sup>SM</sup> 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>.



**PSTA**  
Public Safety Threat Alliance  
Public Safety ISAO

# 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](http://www.motorolasolutions.com).

## OUR VALUES

**WE ARE INNOVATIVE**

**WE ARE PASSIONATE**

**WE ARE DRIVEN**

**WE ARE ACCOUNTABLE**

**WE ARE PARTNERS**

Section 2

# Solution Description

## 2.1 Solution Overview

Motorola Solutions, Inc. (Motorola) is pleased to present the proposed cybersecurity Managed Detection and Response (MDR) services for Nassau County Board of Commissioners (hereinafter referred to as “Customer”).

Identifying and mitigating cyber threats requires a reliable solution that supplies the right data to cybersecurity experts. Motorola will provide access to our ActiveEye<sup>SM</sup> Security Platform, along with 24x7 support from specialized security technologists, who will monitor your mission critical network against threat and intrusion.

The following ASTRO<sup>®</sup> 25 MDR features and services are included in our proposal:

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

### 2.1.1 Site Information

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

**Table 2-1: Site Information**

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

### Services Included

The ActiveEye<sup>SM</sup> 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 Section 3.2.3.3	RNI CEN

## 2.2 Service Description

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

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

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

### 2.2.1 Managed Detection and Response Elements

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

#### 2.2.1.1 ActiveEye<sup>SM</sup> Security Platform

Motorola’s ActiveEye<sup>SM</sup> security platform collects and analyzes security event streams from ActiveEye<sup>SM</sup> 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<sup>SM</sup> platform as part of this service. ActiveEye<sup>SM</sup> will serve as a single interface to display system security information. Using ActiveEye<sup>SM</sup>, the Customer will be able to configure alerts and notifications, review security data, and perform security investigations.

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

### 2.2.1.2 ActiveEye<sup>SM</sup> Managed Security Portal

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



Figure 2-1: ActiveEye<sup>SM</sup> Portal

#### Dashboard

Key information in the ActiveEye<sup>SM</sup> 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<sup>SM</sup> 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<sup>SM</sup> 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<sup>SM</sup> 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<sup>SM</sup> 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<sup>SM</sup> 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<sup>SM</sup> Portal by downloading reports in .csv or .json format.

In addition to *ad hoc* reporting, ActiveEye<sup>SM</sup> 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<sup>SM</sup> 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<sup>SM</sup> 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<sup>SM</sup> Portal provides the ability to add, update, and remove user access. Every ActiveEye<sup>SM</sup> 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.

**2.2.1.3 ActiveEye<sup>SM</sup> 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<sup>SM</sup> platform.

AERSS integrate the ActiveEye<sup>SM</sup> 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

Specifications	Requirements
Current	3.7 A – 7.4 A
Circuit Breaker	Qty. 2
Line Cord	NEMA 5-15P
Heat Dissipation (max)	2107 BTU/hr.
Internet Service Bandwidth	Bandwidth throughput 10Mbps per zone

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

### 2.2.1.4 Internetworking Firewall

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

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

Specifications	Requirement
Rack Space	1U
Power Consumption (Max)	28.6 W (Single Power Supply)
Power Input	100-240V AC
Current	.52 A
Circuits Breaker	Qty. 1
Heat Dissipation (Max)	97.6 BTU/hr.
Line Cord	NEMA 5-15P
Internet Service Bandwidth	Bandwidth throughput 10 MB High availability Internet Connection (99.99% (4-9s) or higher). Packet loss < 0.5%. Jitter <10 ms. Delay < 120 ms. RJ45 Port Speed - Auto Negotiate

## 2.2.2 Service Modules

ActiveEye<sup>SM</sup> delivers service capability by integrating one or more service modules. These modules provide ActiveEye<sup>SM</sup> 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<sup>SM</sup> service module in detail.

### 2.2.2.1 Log Collection / Analytics

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

Collected events will be stored in the ActiveEye<sup>SM</sup> 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.

### 2.2.2.2 Network Detection

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

### 2.2.2.3 External Vulnerability Scanning

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

## 2.2.3 Security Operations Center Services

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

Motorola's SOC is staffed with security experts who will use ActiveEye<sup>SM</sup> 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.

### Section 3

# Statement of Work

## 3.1 Overview

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

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

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

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

## 3.2 Description of Service

### 3.2.1 Deployment Timeline and Milestones

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

#### Phase 1: Service Onboarding

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

The Customer will be provisioned onto the ActiveEye<sup>SM</sup> 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.

### 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<sup>SM</sup> Portal training session.

### Service Commencement

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

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

## 3.2.2 General Responsibilities

### 3.2.2.1 Motorola Responsibilities

- Provide, maintain, and when necessary, repair under warranty hardware and software required to monitor the ASTRO 25 network and applicable CEN systems Inclusive of the AERSS and all software operating on it.
  - If the Centralized Event Logging feature is not installed on the Customer’s ASTRO 25 RNI, Motorola will install it as part of this service.
- Coordinate with the Customer on any system changes necessary to integrate the AERSS into the system and establish necessary connectivity.
- Provide software and licenses to the Customer necessary to remotely monitor the ASTRO 25 network and applicable CEN environments.
- Verify connectivity and monitoring is active prior to start of service.
- Coordinate with the Customer to maintain Motorola service authentication credentials.
- Monitor the Customer’s ASTRO 25 network and applicable CEN systems 24/7/365 for malicious or unusual activity.
- Respond to security incidents in the Customer’s system in accordance with Section 3.3.6: Incident Priority Level Definitions and Response Times. This may include, but is not limited to, requesting additional information from the Customer, continuing to monitor the event for further 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 ActiveEye<sup>SM</sup> platform enabling Customer access to security event and incident details.

### 3.2.2.2 Customer Responsibilities

- The ASTRO 25 MDR service requires a connection from the Customer's ASTRO 25 network and applicable CEN systems to the Internet. Establish connectivity with sufficient bandwidth before service commences. Internet service bandwidth requirements are as follows:
  - Bandwidth throughput of 10MB
  - High availability Internet Connection (99.99% (4-9s) or higher)
  - Packet loss < 0.5%
  - Jitter <10 ms
  - Delay < 120 ms
  - RJ45 Port Speed - Auto Negotiate
- Maintain an active subscription for:
  - Security Update Service (SUS) (or Remote Security Update Service), ensuring patches and antivirus definitions are applied according to the release cadence of the service.
  - ASTRO Dispatch Service and ASTRO Infrastructure Response.

sAllow 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.
- As necessary, upgrade the ASTRO 25 system, on-site systems, and third-party software or tools to supported releases.
- 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.
- Configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a port(s) on a switch) network traffic to the ActiveEye<sup>SM</sup> sensor for applicable CEN systems.
- Respond to Cybersecurity Incident Cases created by the Motorola SOC.



### 3.2.3 Service Modules

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

#### 3.2.3.1 Log Analytics

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

#### Motorola Responsibilities

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

#### Customer Responsibilities

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

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

#### 3.2.3.2 Network Detection

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

#### Motorola Responsibilities

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

#### Customer Responsibilities

- If necessary, configure Customer's networking infrastructure to allow AERSS to communicate with ActiveEye<sup>SM</sup> as defined.

- For Customer's owned CEN infrastructure, configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a port(s) on a switch) network traffic to the ActiveEye<sup>SM</sup> sensor.
- Initiate recommended response actions when active attacks are detected.

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

### 3.2.3.3 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 ActiveEye<sup>SM</sup> portal.
- Create ticket notifications for significant, new findings of interest.

#### Customer Responsibilities

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

Applies to Internet facing assets only.

## 3.3 Security Operations Center Monitoring and Support

### 3.3.1 Scope

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

Motorola's SOC is staffed with security experts who will use ActiveEye<sup>SM</sup> 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<sup>®</sup> 25 MDR service in accordance with Motorola processes and procedures after deployment, as described in Section 3.2.1: Deployment Timeline and Milestones.

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

### 3.3.2 Ongoing Security Operations Center Service Responsibilities

#### Motorola Responsibilities

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

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

#### Customer Responsibilities

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

### 3.3.3 Technical Support

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

## Motorola Responsibilities

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

## 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<sup>SM</sup> Security Management platform and does not include use or implementation of third-party components.

### 3.3.4 Incident Response

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

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

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

#### Motorola Responsibilities

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

### 3.3.5 Event Response and Notification

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

**Table 3-1: Event Handling**

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

#### Notification

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

**Table 3-2: Notification Procedures**

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

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

#### Tuning

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

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

#### Tuning Period Exception

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

responses or notifications may not be delivered. However, Motorola will provide responses and notifications during this period.

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

### 3.3.6 Incident Priority Level Definitions and Response Times

Priority for an alert-generated incident or EOI is determined by the ActiveEye<sup>SM</sup> 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
<b>Critical P1</b>	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: <ul style="list-style-type: none"> <li>• Malware that is not quarantined by anti-virus.</li> <li>• Evidence that a monitored component has communicated with suspected malicious actors.</li> </ul>	Response provided 24 hours, 7 days a week, including US public holidays.
<b>High P2</b>	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: <ul style="list-style-type: none"> <li>• Malware that is quarantined by antivirus.</li> <li>• Multiple behaviors observed in the system that are consistent with known attacker techniques.</li> </ul>	Response provided 24 hours, 7 days a week, including US public holidays.
<b>Medium P3</b>	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: <ul style="list-style-type: none"> <li>• Suspected unauthorized attempts to log into user accounts.</li> <li>• Suspected unauthorized changes to system configurations, such as firewalls or user accounts.</li> <li>• Observed failures of security components.</li> <li>• Informational events.</li> <li>• User account creation or deletion.</li> <li>• Privilege change for existing accounts.</li> </ul>	Response provided on standard business days, Monday through Friday 8:00 a.m. to 5:00 p.m. CST/CDT, excluding US public holidays.

Incident Priority	Incident Definition	Notification Time
Low P4	These are typically service requests from the Customer.	Response provided on standard business days, Monday through Friday from 8:00 a.m. to 5:00 p.m. CST/CDT, excluding US public holidays.

### 3.3.6.1 Response Time Goals

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

### 3.3.6.2 ActiveEye<sup>SM</sup> 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<sup>SM</sup> 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<sup>SM</sup> Platform.

### 3.3.6.3 ActiveEye<sup>SM</sup> 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<sup>SM</sup> 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<sup>SM</sup> Platform which may be impacted by customer configuration changes, telecommunications connectivity, and/or customer network issues/outages.



## Section 4

# Limitations and Clarifications

Motorola's ASTRO MDR service does not include services to perform physical containment and/or remediation of confirmed security incidents, remote or onsite. The Customer may choose to purchase additional Incident Response professional services to assist in the creation of and/or completion of a Customer's Incident Response Plan.

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

## 4.1.1 Service Limitations

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

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

Customer understands and agrees that data obtained, accessed, or utilized in the performance of the services may be transmitted to, accessed, monitored, and/or otherwise processed by Motorola in the U.S. and/or other Motorola operations globally. Customer consents to and authorizes all such processing and agrees to provide, obtain, or post any necessary approvals, consents, or notices that may be necessary to comply with applicable law.

## 4.1.3 Customer and Third-Party Information

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

compromise, and tactics, techniques, and procedures used, learned or developed in the course of providing Services, which data shall be deemed Service Use Data (i.e., Motorola data).

#### **4.1.4 Third-Party Software and Service Providers, including Resale**

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

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

Section 5

# Proposal Pricing

## 5.1 Pricing Summary

### 5.1.1 ASTRO MDR

Motorola pricing is based on the services and solution presented in Section 2. The addition or deletion of any component(s) may subject the total solution price to modifications.

Description	
ASTRO® 25 Managed Detection and Response	\$86,368.00
Hardware and Equipment	Included
Installation and Activation Services	Included
<b>Year 1 Total</b>	<b>\$86,368.00</b>

Initial Subscription Period after Year 1:

Description	
Initial Subscription Period - Year 2	\$46,549.36
Initial Subscription Period - Year 3	\$48,411.33

The Total Contract Value of this proposal is: **\$181,328.69.**

## 5.2 Payment Schedule & Terms

### Period of Performance

The initial MDR subscription period of the contract will extend three (3) years from the Commencement Date of Service, defined as the date data is available for analysis, or not later than thirty (30) days after Motorola provides the Customer with necessary hardware or software.

### Term

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

### Billing

Upon acceptance of this proposal by the Customer, Motorola will invoice the Customer for all service fees in advance for the full Year 1 amount according to the Pricing table in Section 5.1.

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

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

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

**Tax**

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

### 5.3 Invoicing and Shipping Addresses

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

Section 6

# Contractual Documentation

**PRODUCTS AND SERVICES AGREEMENT**

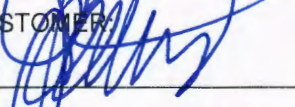
This Products and Services Agreement (this "Agreement") is entered into between **Motorola Solutions Inc.**, ("Seller" or "Motorola") and the entity set forth in section I(b) ("**Customer**") as of the date last signed below ("Effective Date"). Seller and Customer will each be referred to herein as a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

<b>I. Seller and Customer Information</b>		
(a)	Seller	Motorola Solutions, Inc.
(b)	Customer	Name: Nassau County Board of Commissioners  Address: 96135 Nassau Place, Yulee, FL 32097  Contact: Derrick Lindsay

<b>II. Transaction Details</b>		
(a)	Proposal	Proposal No.: <u>24-181900</u> Date: <u>October 8, 2024</u>  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.
(b)	Pricing	Pricing for products and services being purchased by Customer is set forth in the Proposal.
(c)	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.

**III. 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:  
 By:   
 Print Name: John F. Martin, MBA  
 Title: Chairman  
 Date: 12/18/2024

MOTOROLA SOLUTIONS INC.  
 By: Daniel Sanchez  
 Print Name: Daniel Sanchez  
 Title: FL Territory VP  
 Date: 12/3/2024

EXHIBIT A

**GENERAL INFORMATION AND INSURANCE REQUIREMENTS**



**COMMERCIAL GENERAL LIABILITY INSURANCE**

The Vendor/Contractor shall purchase and maintain at the Vendor/Contractor’s expense Commercial General Liability insurance coverage (ISO or comparable Occurrence Form) for the life of this Contract. Modified Occurrence or Claims Made forms are not acceptable.

The Limits of this insurance shall be the following limits:

Each Occurrence Limit	\$1,000,000
Personal & Advertising Injury Limit	\$1,000,000
Products & Completed Operations Aggregate Limit	\$2,000,000
General Aggregate Limit (other than Products & Completed Operations)	\$2,000,000

General liability coverage shall continue to apply to “bodily injury” and to “property damage” occurring after all work on the Site of the covered operations to be performed by the Vendor/Contractor has been completed and shall continue after that portion of “your work” out of which the injury or damage arises has been put to its intended use.

**WORKERS’ COMPENSATION AND EMPLOYER’S LIABILITY INSURANCE**

The Vendor/Contractor shall purchase and maintain at the Vendor/Contractor’s expense Workers’ Compensation and Employer’s Liability insurance coverage for the life of this Contract.

The Limits of this insurance shall be the following limits:

<u>Part One</u> – Workers’ Compensation Insurance – Unlimited	
Statutory Benefits as provided in the Florida Statutes and	
<u>Part Two</u> – Employer’s Liability Insurance	
Bodily Injury By Accident	\$500,000 Each Accident
Bodily Injury By Disease	\$500,000 Policy Limit
Bodily Injury By Disease	\$500,000 Each Employee

\*If leased employees are used, policy must include an Alternate Employer’s Endorsement

**AUTOMOBILE LIABILITY INSURANCE**

The Vendor/Contractor shall purchase and maintain at the Vendor/Contractor’s expense Automobile Liability insurance coverage for the life of this Contract.

The Limits of this insurance shall be the following limits:

Combined Single Limit – Each Accident	\$1,000,000
---------------------------------------	-------------

Covered Automobiles shall include any auto owned or operated by the insured Vendor/Contractor, including autos which are leased, hired, rented or borrowed, including autos owned by their employees which are used in connection with the business of the respective Vendor/Contractor.

**PROFESSIONAL LIABILITY (ERRORS & OMISSIONS)**

This additional coverage will be required for all projects involving consultants, engineering services, architectural or design/build projects, independent testing firms and similar exposures.

The Contractor/Vendor shall purchase and maintain at the Contractor/Vendor’s expense Professional Liability insurance coverage for the life of this Contract.

If the contract includes a requirement for Professional Liability or Errors and Omissions insurance, the amount of such insurance shall be as follows:

Each Claim /Annual Aggregate	\$1,000,000
------------------------------	-------------

EXHIBIT A

Professional Liability coverage will be provided on an Occurrence Form or a Claims Made Form with a retroactive date to at least the first date of this Agreement. If provided on a Claims Made Form, the coverages must respond to all claims reported within three years following the period for which coverage is required and which would have been covered had the coverage been on an occurrence basis.

**CYBER AND DATA SECURITY LIABILITY**

This additional coverage will be required for all projects involving information technology services, software providers, programmers and similar exposures.

The Contractor/Vendor shall purchase and maintain at the Contractor/Vendor’s expense Cyber and Data Security Liability insurance coverage for the life of this Contract.

If the contract includes a requirement for Cyber and Data Security Liability insurance covering Technology Errors & Omissions liability, Media, and Network & Data (Information) Security, the amount of such insurance shall be as follows:

Each Claim / Annual Aggregate \$1,000,000

**Policy coverage must include Third Party Liability coverage.**



Vendor/Contractor shall require each of his Sub-Vendor/Contractors to likewise purchase and maintain at their expense Commercial General Liability insurance, Workers’ Compensation and Employer’s Liability coverage and Automobile Liability insurance coverage meeting the same limit and requirements as the Vendor/Contractors insurance.

**Certificates of Insurance and the insurance policies required for this Agreement shall contain –**

- **The Commercial General Liability, Automobile Liability, and Workers Compensation policies will be endorsed to provide a thirty (30) day notice of cancellation to Nassau County Board of County Commissioners.**
  - **Nassau County Board of County Commissioners must be included as an Additional Insured and endorsed onto the Commercial General Liability (CGL) and Auto Liability policy (ies).**
- **Provision under General Liability, Auto Liability and Workers’ Compensation to include a Waiver of Subrogation clause in favor of Nassau County Board of County Commissioners.**
- **Provision that policies, except Workers’ Compensation and Cyber/Professional, are primary and noncontributory.**

Certificates of Insurance required for this Agreement shall contain a provision under General Liability, Auto Liability, and Workers’ Compensation to include a Waiver of Subrogation clause in favor of Nassau County Board of County Commissioners.

All Insurers must be authorized to transact insurance business in the State of Florida as provided by Florida Statute 624.09(1) and the most recent Rating Classification/Financial Category of the insurer as published in the latest edition of “Best’s Key Rating Guide’ (Property-Casualty) must be at least A- or above.

All of the above referenced Insurance coverage is required to remain in force for the duration of this Agreement and for the duration of the warranty period. Accordingly, at the time of submission of final application for payment, Vendor/Contractor shall submit an additional Certificate of Insurance evidencing continuation of such coverage.

If the Vendor/Contractor fails to procure, maintain or pay for the required insurance, Nassau County Board of County Commissioners shall have the right (but not the obligation) to terminate the Agreement. The failure of Nassau County Board of County Commissioners to demand certificates of insurance and endorsements evidencing the required insurance or to identify any deficiency in Vendor/Contractors coverage based on the evidence of

## EXHIBIT A

insurance provided by the Vendor/Contractor shall not be construed as a waiver by Nassau County Board of County Commissioners of Vendor/Contractor's obligation to procure, maintain and pay for required insurance.

The insurance requirements set forth herein shall in no way limit Vendor/Contractors liability arising out of the work performed under the Agreement or related activities. The inclusions, coverage and limits set forth herein are minimum inclusion, coverage and limits. The required policy limits set forth shall not be construed as a limitation of Vendor/Contractor's right under any policy.. Vendor/Contractor shall be responsible for determining appropriate inclusions, coverage and limits, which may be in excess of the minimum requirements set forth herein.

If the insurance of any Vendor/Contractor or any Sub-Vendor/Contractor contains deductible(s), penalty(ies) or self-insured retention(s), the Vendor/Contractor or Sub-Vendor/Contractor whose insurance contains such provision(s) shall be solely responsible for payment of such deductible(s), penalty(ies) or self-insured retention(s).

The failure of Vendor/Contractor to fully and strictly comply at all times with the insurance requirements set forth herein shall be deemed a material breach of the Agreement.