

Ron DeSantis, Florida Governor
Pedro Allende, Secretary
James Grant, Florida State Chief Information Officer

**AGENCY TERM CONTRACT
FOR
ENDPOINT DETECTION AND RESPONSE
DMS-22/23-155F
BETWEEN
STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES
AND
PRESIDIO NETWORKED SOLUTIONS LLC**

AGENCY TERM CONTRACT

This Contract is between the STATE OF FLORIDA, DEPARTMENT OF MANAGEMENT SERVICES ON BEHALF OF FLORIDA DIGITAL SERVICE (Department), with offices at 4050 Esplanade Way, Tallahassee, Florida 32399-0950, and PRESIDIO NETWORKED SOLUTIONS LLC (Contractor), with offices at 5337 Millenia Lakes Boulevard, Suite 300, Orlando, FL 32839, each a "Party" and collectively referred to herein as the "Parties".

WHEREAS, the Contractor responded to the Department's Request for Quotes (RFQ), No: DMS-22/23-155, Endpoint Detection and Response; and

WHEREAS, the Department has accepted the Contractor's Quote and enters into this Contract in accordance with the terms and conditions of RFQ No. DMS-22/23-155.

NOW THEREFORE, in consideration of the premises and mutual covenants set forth herein, the Parties agree as follows:

1.0 Definitions

- 1.1 Agency Term Contract (ATC or Contract): A written agreement between the Department and the Contractor that is for use by the entire Department and under which Purchase Orders (PO) shall be issued.
- 1.2 Business Day: Any day of the week excluding weekends and holidays observed by State agencies pursuant to subsection 110.117(1)(a)-(j), Florida Statutes (F.S.).
- 1.3 Calendar Day: Any day in a month, including weekends and holidays.
- 1.4 Contract Administrator: The person designated pursuant to section 8.0 of this Contract.
- 1.5 Contract Manager: The person designated pursuant to section 8.0 of this Contract.
- 1.6 Customer: Agencies as defined in section 287.012, Florida Statute (F.S.), and Eligible Users as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.).
- 1.7 Purchaser: The agency, as defined in section 287.012, F.S., or Eligible User, as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.), who issues a Purchase Order from this ATC.

2.0 Scope of Work

The services and/or commodities to be provided by the Contractor pursuant to this Contract are defined and described in Exhibits A and B.

3.0 Contract Term

This ATC shall have an initial term of three (3) years, subject to any limitations based on the term of the underlying Alternate Contract Source (ACS), and shall begin on the last date on which it is signed by all Parties.

4.0 Renewal Terms

The Department reserves the right to renew the Contract in whole or in part, for a renewal term not to exceed three (3) years, or portions thereof, in accordance with section 287.057, F.S. and subject to any limitations based on the term of the underlying ACS, at the renewal pricing specified in the Contractor's Quote or upon mutual agreement of the Parties as set forth in the

Contract. Renewals are also contingent upon satisfactory performance by the Contractor, as determined by the Department.

5.0 Contract Documents and Hierarchy

All Exhibits attached to this Contract are incorporated in their entirety and form as part of this Contract. This Contract sets forth the entire understanding between the Parties and is comprised by the following documents:

1. Exhibit A: RFQ No. DMS-22/23-155.
2. Exhibit B: Contractor's Quote.

In the event that any of the Contract documents conflict, the order of precedence set forth in Section 17.0, of RFQ No. DMS-22/23-155 shall control.

In the event of any conflict between this Contract and any applicable federal or state statute, administrative rule or regulation; the statute, rule or regulation will control.

6.0 Amendments

Unless otherwise provided herein, all modifications to this Contract must be in writing and signed by both Parties, except changes to Section 8.0, below. Any future amendments of the Contract, which alter the definition of the services or scope of work, shall define the services or scope in the same format as Exhibit A and Exhibit B.

Notwithstanding the order listed in Section 5.0, amendments issued after Contract execution may expressly change the provisions of the Contract. If an amendment expressly alters the Contract, then the most recent amendment will take precedence.

7.0 Contract Notices

In addition to the provisions in Section 38 of Form PUR 1000 (10/06), Contract notices may be delivered by email to the Contractor's Representative as prescribed in Section 8.0. All notices by hand-delivery shall be deemed received on the date of delivery, and all notices by email shall be deemed received when they are transmitted and not returned as undelivered or undeliverable.

8.0 Contract Contacts

The Department may appoint a different Contract Administrator or Manager, which will not require an amendment to the Contract, by sending written notice to the Contractor. The Contractor shall address all communication relating to the Contract to the Contract Manager.

8.1 The Department employee who is primarily responsible for maintaining the Contract Administration file is:

Alisha Morgan
Department of Management Services
4050 Esplanade Way
Tallahassee, FL 32399-0950
Email: DMS.Purchasing@dms.fl.gov

The Department's Contract Administrator will perform the following functions:

1. Maintain the official Contract Administration file;
2. Maintain this Contract and all amendments; and
3. Maintain records of all formal contract correspondence between the Department and the Contractor as provided by the Contract Manager for filing in the Contract Administration file.

8.2 The Department's Contract Manager is:

Lacy Perkins
Procurement and Grants Manager
Florida Digital Service
2555 Shumard Oak Blvd.
Tallahassee, FL 32399
Telephone: (850) 274-4156
Email: Purchasing@digital.fl.gov

The Contract Manager will perform the following functions:

1. Maintain a Contract Management file;
2. Serve as the liaison between the Department and the Contractor;
3. Enforce performance of the Contract terms and conditions;
4. Monitor and evaluate the Contractor's performance to ensure services conform to the Contract requirements;
5. Request all amendments, renewals, and terminations of this Contract, and implement management of the Contract change;
6. Exercise applicable remedies, as appropriate, when the Contractor's performance is deficient;
7. Evaluate the Contractor's performance upon completion of this Contract. This evaluation will be placed in the Contract file and will be considered if this Contract is subsequently used as a reference in future procurements.

For each PO issued, the Purchaser's Contract Manager will perform the following functions:

1. Verify the Customer received the deliverables from the Contractor;
2. Review, verify, and approve invoices from the Contractor;
3. Monitor the quality of services and commodities being delivered;
4. Monitor the budget to ensure funds are available through the PO term; and
5. Serve as the liaison between the Department, the Customer, and Contractor relating to quality and delivery.

8.3 The Contractor has assigned the following individual(s) to serve as the Contractor's Representative for this Contract:

Emily Phares
Account Manager
5337 Millenia Lakes Boulevard, Suite 300
Orlando, FL 32839
Telephone: (850) 270-2988
Email: ephares@presidio.com

The Department will direct all questions and customer service issues concerning this Contract to the Contractor's Representative above. It will be the Contractor's Representative's responsibility to coordinate with necessary Department, Purchaser, and Customer personnel, as required, to answer questions and resolve issues. The Contractor must provide written notice to the Department's Contract Manager if a new employee is designated as the Contractor's Representative for this Contract.

9.0 Assignment

The Contractor shall not assign its duties or rights under this Contract to another party without the prior written approval of the Department. The Department shall, at all times, be entitled to assign or transfer its rights, duties, and obligations under this Contract to another governmental agency of the State of Florida upon providing written notice to the Contractor.

10.0 Price Decreases

The Contractor shall apply to the Department any price decrease effectuated during the Contract term by reason of market change or special sales offered to other customers. Such a price decrease applies regardless of whether any related equipment is rented or leased by the Department under the Contract. Price increases are rejected, unless otherwise stated.

11.0 Additions/Deletions

During the term of the Contract, the Department reserves the right to add or delete services and commodities, when considered to be in its best interest and general scope of the Contract. Pricing shall be comparable to the amounts awarded.

12.0 Cooperative Purchasing

Pursuant to their own governing laws, and subject to the agreement of the Contractor, other entities may be permitted to make purchases in accordance with the terms and conditions contained herein. The Department shall not be a party to any transaction between the Contractor and any other purchaser.

13.0 Other Conditions

13.1 Independent Contractor Status

This Contract does not create an employee/employer relationship between the Parties. The Parties are independent contractors under this Contract and neither is the employee of the other for all purposes, including, but not limited to, the application of the Fair Labor Standards Act minimum wage and overtime payments, Federal Insurance Contribution Act, the Social Security Act, the Federal Unemployment Tax Act, the provisions of the Internal Revenue Code, the State Workers' Compensation Act, and the State's unemployment insurance law. The Parties shall each retain sole and absolute discretion in the judgment of the manner and means of carrying out their Contract duties. Services and commodities provided by each Party under this Contract shall be subject to the supervision of the other Party. In performing this Contract, neither Party nor its agents shall act as officers, employees, or agents of the other Party. The Parties agree that they

are separate and independent business enterprises, and that each can pursue other opportunities.

This Contract shall not be construed as creating any joint venture or partnership between the Parties, and neither Party will be liable for any obligation incurred by the other Party, including, but not limited to, unpaid wages and overtime premiums.

13.2 Force Majeure

Neither Party shall be liable for loss or damage suffered as a result of any delay or failure in performance under this Contract or interruption of performance resulting directly or indirectly from acts of God, fire, explosions, earthquakes, floods, water, wind, lightning, civil or military authority, pandemics, acts of public enemy, war, riots, civil disturbances, insurrections, strikes, or labor disputes.

13.3 Cooperation with the Florida Senate and Florida House of Representatives

In accordance with section 287.058(7), F.S., the Contractor agrees to disclose any requested information, relevant to the performance of this Contract, to members or staff of the Florida Senate or Florida House of Representatives, as required by the Florida Legislature. The Contractor is strictly prohibited from enforcing any nondisclosure clauses conflictive with this requirement.

13.4 Employment of State Workers

During the term of the Contract, Contractor shall not knowingly employ, subcontract with or subgrant to any person (including any non-governmental entity in which such person has any employment or other material interest as defined by section 112.312(15), F.S.) who is employed by the State or who has participated in the performance or procurement of this Contract, except as provided in section 112.3185, F.S.

SIGNATURE PAGE IMMEDIATELY FOLLOWS

IN WITNESS THEREOF, the Parties hereto have caused this Contract to be executed by their undersigned officials as duly authorized.

PRESIDIO NETWORKED SOLUTIONS LLC:

STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES:

DocuSigned by:
Erik Hayko
E7A28D0E9E4648D...
Authorized Signature

DocuSigned by:
Pedro Allende
5E01A0D360EB47C...
Pedro Allende, Secretary

Erik Hayko
Print Name

6/29/2023 | 3:36 PM EDT
Date

Senior Contracts Manager
Title

6/29/2023 | 2:50 PM EDT
Date

Exhibit "A"

Request for Quotes (RFQ)

DMS-22/23-155

Endpoint Detection and Response Solution

Alternate Contract Sources:

**Cloud Solutions (43230000-NASPO-16-ACS)
Software Value Added Reseller (SVAR) (43230000-23-NASPO-ACS)
Technology Products, Services, Solutions, and Related Products
and Services (43210000-US-16-ACS)**

1.0 **DEFINITIONS**

The following definitions shall apply throughout this RFQ:

Agency Term Contract (ATC): The written agreement resulting from the award of this Request for Quotes between the Department and the Contractor(s).

Contractor: The vendor awarded an ATC resulting for this Request for Quotes.

Customer: Agencies as defined in section 287.012, Florida Statute (F.S.), and Eligible Users as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.).

Department: The State of Florida, Department of Management Services (DMS), on behalf of the Florida Digital Service (FL[DS]).

Purchase Order: The authorization to begin providing services to a Customer under the terms of this RFQ and a resulting ATC, if applicable.

Purchaser: The agency as defined in section 287.012, F.S., or Eligible User, as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.), who issues a Purchase Order from this RFQ or a resulting ATC.

Quote: A vendor's response to this Request for Quotes.

Solution: An Endpoint Detection and Response (EDR) solution that collects and analyzes endpoint data to detect and respond to cyber security threats.

2.0 **OBJECTIVE**

Pursuant to section 287.056(2), F.S., the Department intends to purchase an EDR (endpoint detection and response) solution for use by the Department and Customers to collect and analyze endpoint data to detect and respond to threats as specified in this RFQ.

The Department also reserves the right to execute an Agency Term Contract (ATC), in the form attached hereto, with the awarded Contractor(s) for the commodities and services specified in this RFQ. The ATC will allow the Department and Customers to purchase the Solution at or below the pricing provided by the awarded Contractor(s) throughout the ATC term.

This RFQ is being issued under the following Alternate Contract Source (ACS) contracts:

- Cloud Solutions (43230000-NASPO-16-ACS)
- Software Value Added Reseller (43230000-23-NASPO-ACS)
- Technology Products, Services, Solutions, and Related Products and Services (43210000-US-16-ACS)

3.0 **DESCRIPTION OF PURCHASE**

The Department is seeking a Contractor(s) to provide an Endpoint Detection and Response (EDR) Solution for the Department and Customers on a statewide basis. The Solution shall include software, implementation, training, support, and integration services as described below. The Contractor will be responsible for providing the Solution to Customers. The Contractor shall be responsible for all aspects of providing the Solution to Customers, as provided herein.

4.0 **BACKGROUND INFORMATION**

In accordance with section 282.318, F.S., the "State Cybersecurity Act," the Department "is the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures." Additionally, the statute states that the Department "shall adopt rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework."

The Department is also responsible for implementing the recommendations of the February 1, 2021, Florida Cybersecurity Task Force Final Report which addresses key objectives related to the state's cybersecurity infrastructure, governance, and operations. The resulting initiatives, projects, and efforts constitute the Enterprise Cybersecurity Resiliency Program.

Additionally, in accordance with section 282.3185, F.S., the "Local Government Cybersecurity Act," "Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework." In the Fiscal Year 2022-2023 General Appropriations Act (line 2944A), the Department was tasked with administering a competitive grant program for local government cybersecurity technical assistance for municipalities and counties. The Department intends to provide access to solutions to equip Customers with resources compliant with the abovementioned cybersecurity standards.

5.0 TERM

The ATC(s) shall have an initial term of three (3) years, subject to any limitations based on the term of the underlying ACS. The Department also reserves the right to renew the ATC(s) in accordance with section 287.057, F.S, and subject to any limitations based on the term of the underlying ACS. Renewals are also contingent upon satisfactory performance by the Contractor, as determined by the Department. Purchase Orders (PO) will be issued in accordance with the RFQ and any applicable ATC as services are needed for Customers. Any POs issued pursuant to the RFQ will have the term identified in the PO.

6.0 SCOPE OF WORK

The Solution proposed in any Quote must not conflict with Chapter 282, F.S., Rule Title 60GG, Florida Administrative Code (F.A.C.), and cybersecurity best practices. The Solution must meet or exceed the applicable state and federal laws, regulations, and standards for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework. The Contractor shall provide services in the manner prescribed by this Scope of Work. The Scope of Work shall be delivered in accordance with the deliverables herein. The Department expects the services to be completed remotely and is not requiring the Contractor to travel. Unless otherwise specified within vendor's Quote, the Solution should include the following items within the Scope of Work, but not be limited to:

6.1. Software Solution/Specifications

The Solution shall detect and respond to threats on endpoint devices such as laptops, desktops, servers, and mobile devices. Endpoint Detection and Response (EDR) solutions typically use a combination of techniques such as behavioral analysis, machine learning, and threat intelligence to identify and respond to security incidents in real-time. The primary purpose of EDR is to detect and respond to advanced threats that have bypassed traditional security defenses such as firewalls and antivirus software. This is accomplished by collecting data from endpoint devices, analyzing it for signs of suspicious activity, and taking automated or manual actions to isolate and neutralize threats. EDR solutions can help organizations improve their overall security posture by providing visibility into the activities taking place on endpoint devices, helping security teams respond to incidents more quickly and effectively, and providing valuable information that can be used to improve security processes and policies.

6.1.1. Multi-Tenant

The Solution shall support a multi-tenant, multi-organization architecture. Each tenant must have its own instance and each instance must aggregate up to a single instance and view. The aggregated instance will support enterprise security operations. The Solution shall provide dashboards for single-source visibility into threats, investigations, and trends.

6.1.2. Scalability

The Solution shall provide the ability to scale to support a large number of tenants and their endpoints.

6.1.3. Cloud Management

The Solution shall be provided as software as a service via cloud-hosted infrastructure to keep current with the latest releases of management server and endpoint agent software. The Solution shall allow capacity extensibility in the cloud with minimal impact on agent or management infrastructure.

6.1.4. Managed Security Services

The Solution shall deploy and maintain managed security services to support Purchasers and Customers, particularly the advanced administration requirement of endpoint detection and response tools and incident response capabilities.

6.1.5. Prevention

The Solution shall block malware pre-execution using the platform's anti-malware prevention program.

6.1.6. Product Usability

The Solution shall provide easy to understand, user-friendly interfaces with intuitive designs to facilitate user engagement, and clear documentation and support resources which instruct on use of the Solution.

6.1.7. Administration and Management Usability

The Solution shall have an easy-to-use administration console and allow straightforward ongoing management that utilizes a lightweight agent with low impact on potential performance.

6.1.8. Endpoint Detection and Response

The Solution shall record system behaviors to detect suspicious events, investigate and block malicious activity, and contain malicious activity at the endpoint. The Solution shall use the data to investigate and provide remediation guidance for any affected systems.

6.1.9. Endpoint Protection Platform Suite

The Solution shall use an extended portfolio of security tools, like endpoint firewalls, device and application control, application inventory, signature matching, vulnerability and patch management and others, plus network-level tools such as secure email and sandboxing.

6.1.10. Operating System Support

The Solution shall protect a wide range of operating systems, including Windows, MacOS and Linux, and mobile operating systems like iOS and Android. The Solution shall provide specific functions for cloud, virtual and container-based workloads.

6.1.11. Data Management and Storage

The Solution shall provide required data storage capacity, file types, and locations, as well as processes such as disaster recovery, rollbacks, extraction, or eradication.

6.1.12. Performance Management

6.1.12.1. The Solution shall provide proactive alerts on system events, as well as logging and resolution reporting on all issues.

6.1.12.2. The Solution shall provide the ability to identify unhealthy agents on endpoints and self-heal issues. Any endpoints that cannot be self-healed must be reported through the administration console and reports.

6.1.13. Security

The Solution shall offer configurable controls that extend data and transaction security and compliance to third-party platforms or hosting providers the Solution uses. The Solution shall document security policies, audits, attestations or evaluations for compliance needs.

6.1.14. Data Management

The Solution shall enable monitoring, reporting, and management of data sharing, as well encryption and security for data at rest and in motion.

6.1.15. Disaster Recovery and Backup

The Solution shall enable processes such as disaster recovery, rollbacks, and version control.

6.1.16. Identity and Access Management

The Solution shall provide capabilities such as user authentication, password policy management, two factor authentication, single sign on, and role-based access.

6.1.17. Network

The Solution shall leverage network technologies like software-defined wide area networks and over-the-top monitoring to ensure the optimal performance of the Solution.

6.1.18. Compliance and Third-Party Certification

The Solution shall comply with relevant standards like General Data Protection Regulation (GDPR), Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act, Personally Identifiable Information (PII)

data requirements, Driver Privacy Protection Act, and third-party certifications such as Systems and Organizations Controls 2 (SOC 2) and International Organization for Standardization (ISO) 27001. The Department, Purchaser, or Customer may require Contractor(s) to execute security agreements, including but not limited to, CJIS riders or Business Associate Agreements as a condition of performance or purchase order issuance.

6.1.19. Configuration and Customization

The Solution shall allow customization of the standard deployed solution with custom user interfaces, data tables, process components, and business logic.

6.1.20. Role-Based Access

The Solution shall provide the ability to create customizable role-based personas based on responsibility.

6.1.21. Data Export

The Solution shall provide the ability to generate a customizable export of data based on user filters for assets, services, and issues present within the platform.

6.1.22. Integration

6.1.22.1. The Solution shall integrate with the Department's existing security tools such as firewalls, antivirus software, endpoint management solutions and security information and event management (SIEM) systems. The Customer shall determine if the Solution is able to integrate with the Customer's security tools. The Contractor shall take any steps necessary to support Customer integration.

6.1.22.2. The Solution shall be capable of data integration through common exchange techniques and frameworks such as RESTful Application Programming Interfaces (APIs).

6.1.22.3. The Solution shall be capable of integrating with a variety of identity and access management (IAM) systems to meet Customer current and future needs.

6.1.22.4. Initial Integration shall include connecting each Customer to the state Cybersecurity Operations Center (CSOC) and validating with FL[DS] that all Solution data is properly integrated, as requested by the Customer.

6.1.22.5. Integration Maintenance may be required after initial integration to ensure that the Solution properly exchanges data between Customers and the CSOC. The Contractor shall address any concerns that FL[DS] has regarding integration issues.

6.1.23. Performance and Availability

The Solution shall perform in accordance with the approved Service Level Agreement (SLA) (see Section 10.2) and be available 99.999% of the time per month.

6.1.23.1. The performance and availability SLA shall provide information on performance and availability objectives for the Solution to perform successfully and be available 99.999% of the time per month.

6.1.23.2. The vendor shall propose meaningful financial consequences in the draft performance and availability SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.2. Training and Support

Through the Solution, the Contractor shall provide all consulting, training, and support to the Customer and FL[DS] to ensure successful implementation of the Solution and ongoing support as necessary and as defined by FL[DS] to include, but not be limited to:

6.2.1. Consult with and the Department, the Purchaser, and the Customer to ensure the Department, the Purchaser, and the Customer have the information necessary for decision-making.

6.2.2. Adhere to the FL[DS]-approved training SLA that specifies the objectives, description of the materials/resources provided to meet the objectives, suggested method of training (in-person, live webinar, online course, etc.), and specific training suggested for each user roles.

6.2.2.1. The training SLA must specify Initial Training (included in Item No. 1 on Attachment A, Price Sheet) provided and Ongoing Training provided (included in Item No. 2 on Attachment A, Price Sheet).

6.2.2.2. The vendor shall propose meaningful financial consequences in the draft training SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.2.3. Adhere to the FL[DS]-approved SLA for support service which provides information on support objectives, resources, availability, response times, resolution times and issue criticality levels.

6.2.3.1. The vendor shall propose meaningful financial consequences in the draft support service SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.3. Kickoff Meeting

6.3.1. The Contractor shall conduct a kickoff meeting with the Purchaser to further clarify PO expectations.

6.3.2. If the PO covers more than just the Purchaser, the Contractor shall conduct a kickoff meeting for each Customer on a date and time agreed upon by the FL[DS] (if the Solution is being integrated into the CSOC) and the Customer.

The Contractor may hold a kickoff meeting with multiple Customers per meeting.

- 6.3.3. The kickoff meeting for the Customer should include a demonstration of the Solution, or prior to the kickoff meeting, a link may be provided to the Customer to demonstrate the Solution.

6.4. **Implementation**

The Contractor shall implement the Solution with each Customer upon the Purchaser's approval, FL[DS] approval (if the Solution is integrating with the CSOC), and the Customer's approval of the Implementation Plan. The Contractor shall collaborate with the Customer to develop an Implementation Plan addressing all items contained in **Section 6.0**, Scope of Work, and submit it to the Purchaser, FL[DS] as applicable, and the Customer for approval.

The Implementation Plan must include the following at a minimum:

- 6.4.1. All tasks are required to fully implement and complete Initial Integration of the Solution.
- 6.4.2. Identify if the Contractor, Purchaser, FL[DS] (if applicable), or other Customer is responsible for each task.
- 6.4.3. Dates that each task (or group of tasks) will be completed by, identify task dependencies, and tasks on the critical path to ensure timely project completion.
- 6.4.4. Describe necessary training, method of training (e.g., in-person, live webinar, online course), and training dates.
- 6.4.5. Describe the support available to ensure successful implementation and Initial Integration.
- 6.4.6. Provide Contractor contact information (name, title, email, and phone number) for the Contractor Representative who is assigned to oversee successful implementation and Initial Integration.
- 6.4.7. Document the frequency and method(s) for the Contractor to communicate the ongoing status of the Implementation Plan to the Purchaser and any other Customers.

6.5. **Reporting**

The Contractor shall provide the following reports to the Purchaser:

- 6.5.1. Quarterly Business Reviews (QBR) which will include, but not be limited to, performance reports and metrics on service level achievements. The Contractor shall schedule a quarterly meeting to review the QBR and document any financial consequences to be assessed as necessary.
- 6.5.2. Monthly Implementation Reports shall be provided to the Purchaser to document compliance with Final Implementation Plan(s) and document any financial consequences to be assessed as necessary.

- 6.5.3. Monthly Training Reports shall be provided to the Purchaser to document all training provided to the Purchaser and any other Customers and document any financial consequences to be assessed as necessary.
- 6.5.4. Monthly Service Reports shall be provided to the Purchaser to document Solution performance, availability, response times, and resolution times and document any financial consequences to be assessed as necessary.
- 6.5.5. Ad hoc reports as requested by the Purchaser.

6.6. Optional Services

6.6.1. Manage, Detect, and Respond (MDR)

If available, the vendor shall provide optional annual pricing along with an SLA to manage, detect, and respond to security issues detected by the Solution.

- 6.6.1.1. Adhere to the FL[DS]-approved MDR SLA which provides information on MDR objectives, resources, availability, response times, resolution times, and issue criticality levels.
- 6.6.1.2. The vendor shall propose meaningful financial consequences in the draft MDR SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.6.2. Future Integrations

If available, the vendor shall provide optional pricing along with an SLA for Application Programming Interfaces available for the Solution.

- 6.6.2.1. Adhere to the FL[DS]-approved SLA for future integrations which include services and solutions that augment, enhance, or expand the Solution in a meaningful way.
- 6.6.2.2. The vendor shall propose meaningful financial consequences in the draft future integrations SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

7.0 DELIVERABLES

Deliverables for each Purchase Order may be submitted earlier than the delivery dates listed in **Table 1**. All deliverables are subject to the approval and acceptance of the Purchaser. The Contractor shall provide the services identified in **Section 6.0**, Scope of Work, to complete the deliverables as described in **Table 1** below. The Contractor will not be compensated for the kickoff meetings, or any work performed before or during the development of the Implementation Plan. Once the Implementation Plan is approved in writing by the Purchaser, FL[DS] (if applicable), and the Customer, as applicable, the Contractor shall provide the Customer with access to the software in accordance with the approved Implementation Plan (Final Implementation Plan). Once software access is granted to the Customer, and the Customer confirms receipt, the Contractor will invoice the Purchaser at the pricing established in Attachment A, Price Sheet, within thirty (30) days. The Contractor will be compensated, annually, in advance, for the Solution for each PO in accordance with this RFQ. The Purchaser may waive or amend any due dates in writing at its sole discretion.

**TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES**

No.	Deliverable	Time Frame	Financial Consequences
1	The Contractor shall host a kickoff meeting with the Purchaser individually, and kickoff meeting with each additional Customer, and FL[DS] (if applicable) in accordance with the PO, and any applicable ATC.	The Contractor shall host the meeting within five (5) calendar days of PO issuance.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after deliverable due date.
2	The Contractor shall submit the Implementation Plan timely and in accordance with the PO and any applicable ATC.	The Contractor shall collaborate with the Customer and submit each Customer's Implementation Plan to the Purchaser and each additional Customer within 10 calendar days of PO issuance.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after the deliverable due date until the Customer Implementation Plan is received. Financial consequences shall also be assessed for a Customer's Implementation Plan submitted that is not in accordance with the PO and any applicable ATC, in the amount of \$500 for each incomplete Implementation Plan.
3	The Contractor shall provide Solution access and all services in the Final Implementation Plan in accordance with this PO and any applicable ATC.	The Contractor shall provide Solution access and complete all requirements established in the Final Implementation Plan timely and accurately.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after any due date specified in the Final Implementation Plan, until the requirement is accurately completed. Financial consequences shall be assessed in the amount of \$200 per requirement for each instance services are not performed, or documentation is not received, in accordance with this RFQ and the Implementation Plan.

**TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES**

No.	Deliverable	Time Frame	Financial Consequences
4	The Contractor shall ensure the Solution is available in accordance with this PO and any applicable ATC.	The Solution must be available 99.999% of the time per month in accordance with the FL[DS]-approved SLA and. Compliance is calculated on a monthly basis for each Customer.	Financial Consequences shall be assessed against the Contractor in the amount of \$100 for each negative deviation from the thousandth decimal point. For example, a Customer's monthly uptime of 99.997% will result in a financial consequence of \$200, unless the Department accepts different financial consequence in the Contractor's Quote.
5	The Contractor shall ensure the Solution performs in accordance with the FL[DS]-approved SLA.	The Solution must perform in accordance with the FL[DS]-approved SLA.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after any due date specified in the FL[DS]-approved SLA, until the requirement is accurately completed, unless the Department accepts different financial consequence in the Contractor's Quote.
6	The Contractor shall ensure training and support are provided in accordance with the FL[DS]-approved SLA.	Training and support must be provided in accordance with Section 6.2. of this RFQ and the FL[DS]-approved SLA for training and support.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after any due date specified in the FL[DS]-approved SLA, until the requirement is accurately completed, unless the Department accepts different financial consequence in the Contractor's Quote.

**TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES**

No.	Deliverable	Time Frame	Financial Consequences
7	The Contractor shall report accurate information in accordance with the PO and any applicable ATC.	<p>QBRs are due 15 calendar days after the end of the quarter (January - March, April - June, July - September, and October - December).</p> <p>Monthly Implementation Reports are due five (5) calendar days after the end of the month.</p> <p>Monthly Training Reports are due five (5) calendar days after the end of the month.</p> <p>Monthly Service Reports are due five (5) calendar days after the end of the month.</p> <p>Ad hoc reports are due five (5) calendar days after the request by the Purchaser.</p>	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after any due date, until an accurate report is received.

All deliverables are subject to the approval and acceptance of the Purchaser. Any deliverables rejected by the Purchaser will be subject to the applicable financial consequences in Table 1 until the Contractor resubmits and the Purchaser accepts the deliverable.

8.0 PERFORMANCE MEASURES

The Contractor shall perform all required services in a proper and satisfactory manner as determined by the Purchaser. The Contractor shall perform 100% of deliverable requirements to the satisfaction of the Purchaser, within the PO-required deadlines.

8.1 Performance Compliance

By submitting a response to this RFQ, the Contractor acknowledges and agrees that its performance under this SOW must meet the standards set forth above and that it will be bound by the conditions set forth herein. After executing an applicable financial consequence, the Purchaser may, at its sole discretion, allow additional time for the

Contractor to remedy the performance issues identified by the Purchaser; or, after giving the Contractor a reasonable opportunity to cure such performance issues, may proceed with default proceedings.

The Purchaser reserves the right to perform or assign the required services to another contractor, if the awarded Contractor is not achieving the required levels of service, after the Contractor has been duly notified of their inadequacy.

Where any applicable ATC(s) and PO(s) require the generation and submission of deliverables to the Purchaser, receipt by the Purchaser will not be construed to mean or imply acceptance of those deliverables. It is specifically intended by the Purchaser that acceptance of required deliverables constitute a separate act. The Purchaser may reject deliverables as incomplete, inadequate, or unacceptable according to the parameters set forth in this SOW.

By submitting a Quote, the vendor represents and warrants that the Solution substantially conforms or exceeds the specifications herein and will continue to substantially conform or exceed the specifications provided herein throughout the duration of any resultant ATC and PO. The Solution's failure to substantially conform or exceed these specifications may result in termination of any resultant ATC or PO(s).

9.0 FINANCIAL CONSEQUENCES

The Purchaser shall impose financial consequences upon the Contractor for failure to comply or submit evidence documenting compliance with the performance standard requirements, or deliverable deemed unacceptable by the Purchaser if the Contractor fails to resolve errors, as set forth in **Section 7.0**, Deliverables. If the Purchaser chooses to allow completion of Contract requirements after the time allowed, its allowance shall not act as a waiver of financial consequences. These financial consequences are not a penalty and are intended to incentivize successful performance of the specified requirements.

The financial consequences assessed will result in a payment or an automatic credit to the Purchaser, at the Purchaser's discretion. In the event the Purchaser disagrees with a financial consequence assessment by the Contractor, the Purchaser will make the final determination on the Contractor's compliance with the deliverables and financial consequence assessment.

10.0 RESPONSE CONTENT AND FORMAT

10.1 Responses are due by the date and time shown in **Section 11.0**, Timeline.

10.2 Quotes shall be concise, in an electronic Adobe PDF format, and prepared using the following outline:

- 1) Documentation to describe the endpoint detection and response Solution proposed and how it meets the requirements of this RFQ to include the following at a minimum:
 - a. A draft SLA for Solution performance and availability which adheres to all provisions of this RFQ.
 - b. A draft SLA for training and support which adheres to all provisions of this RFQ.

- i. The training SLA must specify initial training (included in Item No. 1 on Attachment A, Price Sheet) provided and ongoing training provided (included in Item No. 2 on Attachment A, Price Sheet).
 - c. A draft implementation plan for a Customer which adheres to all provisions of this RFQ.
 - d. A draft MDR SLA, if applicable, per section 6.6.1 with annual pricing.
 - e. A draft SLA for future integrations, if applicable, per section 6.6.2 with pricing.
 - f. A draft disaster recovery plan per section 32.5.
- 2) Documentation describing any experience providing the Solution, or similar Solution, on a statewide basis or across a large geographic region.
 - 3) Documentation describing the vendor's capacity and ability to implement the Solution on a statewide basis.
 - 4) Detail regarding any value-added services.
 - 5) **Attachment A**, Price Sheet, containing pricing for all items and completed in accordance with the instructions provided in this RFQ.
 - 6) **Attachment B**, Contact Information Sheet, containing the contacts for the Quote and the resulting ATC(s) and PO(s).
 - 7) **Non-Disclosure Agreement** executed by the vendor.

If the vendor is utilizing subcontractors, the vendor shall identify all subcontractors the vendors will utilize to provide the services required by this RFQ and what services each subcontractor will provide.

10.3 All Quotes should be submitted via email to the Department's Procurement Officer, identified in **Section 12.0**. Quotes must remain valid for at least 180 calendar days.

Note: If the vendor considers any part of its response to the RFQ to be trade secret or otherwise confidential or exempt from disclosure under Florida or federal law ("Confidential Information"), it shall provide the Department with a copy of its response with such Confidential Information redacted in accordance with Section 19.

11.0 **TIMELINE**

EVENT	DATE
Release of the RFQ	May 10, 2023
Pre-Quote Conference Registration Link: https://us02web.zoom.us/meeting/register/tZMrf-2qqTgtEtUhsUQg5jjxixaUSqJ9oFLS	May 15, 2023, at 2:00 p.m., Eastern Time
Responses Due to the Procurement Officer, via email	May 19, 2023, by 5:00 p.m., Eastern Time
Solution Demonstrations and Quote Negotiations	May 22-24, 2023
Anticipated Award, via email	May 24, 2023

12.0 PROCUREMENT OFFICER

The Procurement Officer for this RFQ is:

Alisha Morgan
Department of Management Services
4050 Esplanade Way
Tallahassee, FL 32399-0950
DMS.Purchasing@dms.fl.gov

13.0 PRE-QUOTE CONFERENCE

The Department will hold a Pre-Quote Conference as indicated in **Section 11.0**, Timeline, above to answer vendor questions. The Department will use its best efforts to answer vendor questions during the Pre-Quote Conference.

14.0 SOLUTION DEMONSTRATIONS

If the Department requests a demonstration of the Solution, the vendor must be available to demonstrate the Solution to the Department during the timeframe specified in **Section 11.0**, Timeline.

15.0 QUOTE NEGOTIATIONS

The Department may schedule negotiation sessions with vendors to discuss the Quote if any aspects of the Quote are not in the best interest of the Department. These negotiations will be scheduled in the timeframe specified in **Section 11.0**, Timeline. The Department does not anticipate exceeding these timeframes. The Department may require the vendors to revise any terms and conditions in the vendor's Quote, including any SLAs, during this timeframe.

16.0 SELECTION OF AWARD

The Department intends to select one (1) or more vendor(s) that provide the overall best value to the State. The Department will consider all aspects of submitted Quotes when making a selection, including the proposed Solution, how it meets the requirements, benefits to the State, and price.

17.0 RFQ HIERARCHY

The ATC(s) and PO(s) resulting from this RFQ will include the following Attachments which set forth the entire understanding of the Customer, the Contractor, and the Department and supersede all prior agreements. All Attachments listed below will be incorporated in their entirety into, and form part of any ATC(s) or PO(s) issued. In the event of a conflict between the documents that make up any ATC(s) and PO(s), priority shall be in the order listed:

- 1) The PO(s);
- 2) The ATC(s);
- 3) The Department's Non-Disclosure Agreement (NDA) or other Purchaser's NDA;
- 4) This RFQ;
- 5) Department's Purchase Order Terms and Conditions;
- 6) The ACS contract the vendor submitted their Quote in accordance with [ACS: Cloud Solutions (43230000-NASPO-16-ACS), Software Value Added Reseller (SVAR) (43230000-23-NASPO-ACS), or Technology Products, Services, Solutions, and Related Products and Services (43210000-US-16-ACS)]; and
- 7) The vendor's Quote.

18.0 DEPARTMENT'S CONTRACT MANAGER

The Department's Contract Manager who will oversee the Contractor's performance of its duties and obligations pursuant to the terms of any applicable ATC and any resultant PO and serve as a liaison with the Contractor, will be as follows:

To Be Determined
Florida Department of Management Services
Florida Digital Service
2555 Shumard Oak Blvd
Tallahassee, FL 32399
purchasing@digital.fl.gov

19.0 PAYMENT

- 19.1** The Contractor will be compensated in advance, annually, for all Deliverables per PO. Once the Implementation Plan is approved by the Purchaser, FL[DS] (if applicable) and the Customer in writing, the Contractor shall provide the Customer with access to the software in accordance with the Final Implementation Plan. Once software access is granted to the Customer, and the Customer confirms receipt, the Contractor will submit one (1) invoice to the Contract Manager specified in the PO indicating the date the Customer received the software access.
- 19.2** On each invoice, the Contractor shall certify that all costs and fees claimed in the invoice statement for payment are accurate and were performed in furtherance of the PO.
- 19.3** Contractor compensation will be exclusively made in accordance with the terms of this RFQ, any applicable ATC, and the PO. The Purchaser will not reimburse the Contractor for any other expenses associated with, or related to, any applicable ATC or resultant PO(s). For example, travel related expenses, including lodging, mileage, vehicle rental, and food, will not be subject to reimbursement.
- 19.4** Purchasers shall pay invoices in accordance with their governing laws and regulations, which shall govern the rights and obligations of the Purchaser and the Contractor. The Department shall pay invoices submitted by the Contractor in accordance with the provisions of section 215.422, F.S., which shall govern the rights and obligations of the Department and the Contractor.
- 19.5** The Contractor is responsible for the performance of all tasks and deliverables contained in any applicable ATC or PO.

20.0 PUBLIC RECORDS AND DOCUMENT MANAGEMENT

20.1 Access to Public Records

The Department may unilaterally cancel any applicable ATC or PO for failure by the Contractor to comply with this section by not allowing access to all public records, as defined in Chapter 119, F.S., made or received by the Contractor in conjunction with any applicable ATC or PO.

20.2 Contractor as Agent

Solely for the purposes of this section, the Contract Manager specified in the PO is the custodian of public records. If under the PO, the Contractor is providing services and is acting on behalf of a public agency, as provided by section 119.0701, F.S., the Contractor shall:

- 1) Keep and maintain public records required by the public agency to perform the service.
- 2) Upon request from the public agency's custodian of public records, provide the public agency with a copy of the requested records or allow the records to be inspected or copied within a reasonable time and at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law.
- 3) Ensure that public records that are exempt or confidential and exempt from public records disclosure are not disclosed except as authorized by law for the duration of the PO term and following the completion of the PO if the Contractor does not transfer the records to the public agency.
- 4) Upon completion of the PO, transfer, at no cost, to the public agency all public records in possession of the Contractor or keep and maintain public records required by the public agency to perform the service. If the Contractor transfers all public records to the public agency upon completion of the PO, the Contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of the PO, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the Purchaser, upon request from the Purchaser's custodian of public records, in a format that is compatible with the information technology systems of the Purchaser.
- 5) **IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, F.S., TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THE PURCHASE ORDER, CONTACT THE FOLLOWING CONTACTS:**

DEPARTMENT:

CUSTODIAN OF PUBLIC RECORDS

PHONE NUMBER: 850-487-1082

EMAIL: PublicRecords@dms.fl.gov

**MAILING ADDRESS: 4050 ESPLANADE WAY, SUITE 160
TALLAHASSEE, FL 32399.**

OTHER PURCHASER:

CONTRACT MANAGER SPECIFIED ON THE PO

20.3 Public Records Exemption

The Contractor may have access to cybersecurity information classified as confidential and exempt under section 119.0725, F.S. In the event that the Contractor has access to confidential and exempt information, the Contractor agrees to maintain the confidentiality as required in section 119.0725, F.S.

20.4 Document Management

The Contractor must retain sufficient documentation to substantiate claims for payment under the PO and all other records, electronic files, papers, and documents that were made in relation to the PO. The Contractor must retain all documents related to the PO for five (5) years after the expiration of the PO, or, if longer, the period required by the General Records Schedules maintained by the Florida Department of State available at the Department of State's Records Management website.

21.0 IDENTIFICATION AND PROTECTION OF CONFIDENTIAL INFORMATION

Article 1, section 24, Florida Constitution, guarantees every person access to all public records, and section 119.011, F.S., provides a broad definition of "public records." As such, records submitted to an Agency as defined in section 119.011, F.S. (referred to for purposes of this Section 19 as "Agency") are public records and are subject to disclosure unless exempt from disclosure by law. If the vendor considers any portion of records it provides to an Agency (including those submitted in response to this RFQ) to be trade secret or otherwise confidential or exempt from disclosure under Florida or federal law ("Confidential Information"), the vendor shall mark the document as "confidential" and simultaneously provide that Agency with a separate, redacted copy of the record. For each portion redacted, the vendor should briefly describe in writing the grounds for claiming exemption, including the specific statutory citation for such exemption. The vendor shall only redact portions of records that it claims are Confidential Information.

In the event of a request for public records pursuant to Chapter 119, F.S., the Florida Constitution, or other authority, to which records that are marked as "confidential" are responsive, the Agency will provide the vendor-redacted copy to the requestor. If a requestor asserts a right to the redacted Confidential Information, the Agency will notify the vendor such an assertion has been made. It is the vendor's responsibility to take the appropriate legal action to assert that the information in question is exempt from disclosure under Chapter 119, F.S., or other applicable law.

If the Agency becomes subject to a demand for discovery or disclosure of documents that are marked as "confidential" in a legal proceeding, the Agency will give the vendor notice of the demand or request. The vendor shall take the appropriate legal action in response to the demand and to defend its claims of confidentiality. If the vendor fails to take appropriate and timely action to protect the records it has designated as Confidential Information, the Agency will provide the unredacted records to the requester.

The vendor shall protect, defend, and indemnify the Agency and any applicable Customer for all claims, costs, fines, and attorneys' fees arising from or relating to the vendor's determination that the redacted portions of its records are Confidential Information. If the vendor fails to submit a redacted copy in accordance with this section, of information it claims is Confidential Information, the Agency is authorized to produce the entire record submitted to the Agency in response to a public records request for, or demand for discovery or disclosure of, these records.

22.0 USE OF SUBCONTRACTORS

In providing services under the PO(s) and any applicable ATC, the Contractor is permitted to utilize subcontractors identified in its Quote. The Contractor shall notify the Contract Manager specified on the PO in writing of any subcontractors not identified in the Contractor's Quote who will be engaged to provide services for a PO 10 calendar days prior to their engagement.

During the term of the PO, subcontractors may be substituted with the prior written approval of the Contract Manager specified on the PO. The Purchaser reserves the right to reject a subcontractor with 10 calendar days advance notification to the Contractor.

The Contractor is fully responsible for the satisfactory completion of all subcontracted work and is required to ensure subcontractor's adherence to the terms set forth any PO.

The Contractor shall make all payments to subcontractors. If the Contractor utilizes a subcontractor, the Contractor shall pay the subcontractor within seven (7) Business Days after any payment is received from the Purchaser, per section 287.0585, F.S. It is understood, and agreed upon, that the Department shall not be held accountable to any subcontractor for any expenses or liabilities incurred under the subcontract, and that the Contractor is solely responsible to the subcontractor for all expenses and liabilities under the Contract. If the Contractor fails to pay the subcontractor within seven (7) Business Days, the Contractor shall pay the penalty to the subcontractor in the amount of one-half (1/2) of one percent (1%) of the amount due, per Calendar Day, from the expiration of the period allowed herein for payment. Such penalty shall be in addition to actual payments owed and shall not exceed 15% of the outstanding balance due.

23.0 LEGISLATIVE APPROPRIATION

Pursuant to section 287.0582, F.S., the State of Florida's performance and obligation to pay under any PO is contingent upon an annual appropriation by the Legislature.

24.0 MODIFICATIONS

The Department reserves the right to change, add or delete any requirement from this RFQ if the Department deems it to be in the best interest of the State of Florida. In addition, the Department reserves the right to withdraw and cancel this RFQ at any time, prior to a duly authorized and executed ATC or PO.

25.0 CONFLICT OF INTEREST

It is essential that the vendor and any subcontractors are independent and impartial and that the implementation of decisions made as it relates to consultation and services is not used for private gain or other remuneration. The Contractor shall not receive any monies for services provided under the PO aside from those paid pursuant to the PO.

26.0 DISCRIMINATORY, CONVICTED AND ANTITRUST VENDORS LISTS

The vendor is hereby informed of the provisions of sections 287.133(2)(a), 287.134(2)(a), and 287.137(2)(a), F.S., that identify the impacts to the vendor 's ability or its affiliates' ability to respond to the competitive solicitations of a public entity; to be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with a public entity; or to transact business with a public entity if it, or its affiliates, are placed on the Convicted Vendor, Discriminatory Vendor, or Antitrust Violator Vendor Lists of the Department of Management Services. The Contractor shall promptly notify the Purchaser if it or its suppliers, subcontractors, or consultants under any POs are placed on any such lists.

27.0 E-VERIFY

The Contractor (and its subcontractors) has an obligation to utilize the U.S. Department of Homeland Security's (DHS) E-Verify system for all newly hired employees in accordance with section 448.095, F.S. By accepting the ATC or any PO(s), the Contractor certifies that it is registered with, and uses, the E-Verify system for all newly hired employees in accordance with section 448.095, F.S. The Contractor must obtain an affidavit from its subcontractors in

accordance with paragraph (2)(b) of section 448.095, F.S., and maintain a copy of such affidavit for the duration of any applicable ATC(s) and any PO(s). The Contractor shall provide a copy of its DHS Memorandum of Understanding (MOU) to the Contract Manager specified on the PO within five (5) business days of issuance of the ATC or any PO(s). The Contract Manager will be designated on any applicable ATC and PO.

This section serves as notice to the Contractor regarding the requirements of section 448.095, F.S., specifically sub-paragraph (2)(c)1, and the Department's obligation to terminate the ATC and any other Purchaser's obligation to terminate any PO(s) if it has a good faith belief that the Contractor has knowingly violated section 448.09(1), F.S. If terminated for such reason, the Contractor will not be eligible for award of a public contract for at least one (1) year after the date of such termination. The Department or any other applicable Purchaser will promptly notify the Contractor and order the immediate termination of any contract between the Contractor and a subcontractor performing work on its behalf under the ATCs and any PO(s) should the Department or any other applicable Purchaser develop a good faith belief that the subcontractor has knowingly violated section 448.095(1), F.S.

28.0 COOPERATION WITH INSPECTOR GENERAL

Pursuant to section 20.055(5), F.S., Contractor, and its subcontractors (if any), understand and will comply with their duty to cooperate with the Department's or any Purchaser's Inspector General in any investigation, audit, inspection, review, or hearing.

29.0 ACCESSIBILITY

The Contractor will comply with section 508 of the Rehabilitation Act of 1973, as amended and 29 U.S.C. s. 794(d), including the regulations set forth under 36 C.F.R. part 1194. Section 282.601(1), F.S., states that "state government shall, when developing, competitively procuring, maintaining, or using electronic information or information technology acquired on or after July 1, 2006, ensure that State employees with disabilities have access to and are provided with information and data comparable to the access and use by State employees who are not individuals with disabilities."

30.0 PRODUCTION AND INSPECTION

In accordance with section 216.1366, F.S., any public agency is authorized to inspect the: (a) financial records, papers, and documents of the contractor that are directly related to the performance of the contract or the expenditure of state funds; and (b) programmatic records, papers, and documents of the contractor which the public agency determines are necessary to monitor the performance of the contract or to ensure that the terms of the PO are being met. The Contractor shall provide such records, papers, and documents requested by the public agency within 10 business days after the request is made.

31.0 SCRUTINIZED COMPANIES

In accordance with the requirements of section 287.135(5), F.S., the vendor certifies that it is not participating in a boycott of Israel. At the Department's or Purchaser's option, any applicable ATC or PO may be terminated if the Contractor is placed on the Quarterly List of Scrutinized Companies that Boycott Israel (referred to in statute as the "Scrutinized Companies that Boycott Israel List") or becomes engaged in a boycott of Israel. The State Board of Administration maintains the "Quarterly List of Scrutinized Companies that Boycott Israel" at the following link:

<https://www.sbafla.com/fsb/FundsWeManage/FRSPensionPlan/GlobalGovernanceMandates.aspx>.

32.0 BACKGROUND SCREENING

All Contractor employees and their subcontractors and agents performing work under the Contract must comply with all security and administrative requirements of the Department and the Purchaser.

32.1 Background Check

In addition to any background screening required by the Contractor as a condition of employment, the Contractor warrants that it will conduct a criminal background screening of, or ensure that such a screening is conducted for, each of its employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees or other person, hereinafter referred to as "Person" or "Persons," operating under their direction who directly perform services under the Contract, whether or not the Person has access to State of Florida Data, as well as those who have access, including indirect access, to State of Florida Data, whether or not they perform services under the PO. The Contractor warrants that all Persons will have passed the Background Screening described herein before they have Access to Data or begin performing services under the Contract. The look-back period for such background screenings shall be for a minimum of six years where six years of historical information is available.

"Access" means to review, inspect, approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any data, regardless of type, form, or nature of storage. Access to a computer system or network includes local and remote access.

"Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions, whether it is exempt, confidential, or personal health information. Data may be in any form, including but not limited to, storage media, computer memory, in transit, presented on a display device, or in physical media such as paper, film, microfilm, or microfiche. Data includes the original form of the Data and all metadata associated with the Data.

The minimum background check process will include a check of the following databases through a law enforcement agency or a Professional Background Screener accredited by the National Association of Professional Background Screeners or a comparable standard:

- 1) Social Security Number Trace; and
- 2) Criminal Records (Federal, State and County criminal felony and misdemeanor, national criminal database for all states which make such data available).

32.2 Disqualifying Offenses

If at any time it is determined that a Person has a criminal misdemeanor or felony record regardless of adjudication (e.g., adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict) within the last six years from the date of the court's determination for the crimes listed below, or their equivalent in any jurisdiction, the Contractor is required to immediately remove that Person from any position with

access to State of Florida Data or directly performing services under the Contract. The disqualifying offenses are:

- 1) Computer related or information technology crimes;
- 2) Fraudulent practices, false pretenses and frauds, and credit card crimes;
- 3) Forgery and counterfeiting;
- 4) Violations involving checks and drafts;
- 5) Misuse of medical or personnel records; or
- 6) Felony theft.

If the Contractor finds a Disqualifying Offense for a Person within the last six years from the date of the court's disposition, it may obtain information regarding the incident and determine whether that Person should continue providing services under the Contract or have access to State of Florida Data. The Contractor will consider the following factors only in making the determination: i.) nature and gravity of the offense, ii.) the amount of time that has elapsed since the offense, iii.) the rehabilitation efforts of the person, and iv.) relevancy of the offense to the job duties of the Person. If the Contractor determines that the Person should be allowed access to State of Florida Data, then Contractor shall maintain all criminal background screening information and the rationale for such access in the Person's employment file.

32.3 Refresh Screening

The Contractor will ensure that all background screening will be refreshed every five (5) years from the time initially performed for each Person during the Term of the Contract.

32.4 Self-Disclosure

The Contractor shall ensure that all Persons have a responsibility to self-report within three calendar days to the Contractor any updated court disposition regarding any disqualifying offense, regardless of adjudication (adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict). The Contractor shall immediately reassess whether to disallow that Person access to any State of Florida premises or from directly performing services under the Contract. Additionally, the Contractor shall require that the Person complete an annual certification that they have not received any additional criminal misdemeanor or felony record regardless of adjudication (adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict) for the Disqualifying Offenses and shall maintain that certification in the employment file.

In addition, the Contractor shall ensure that all Persons have a responsibility to self-report to the Contractor within three calendar days, any arrest for any Disqualifying Offense. The Contractor shall notify the Contract Manager specified on the PO and any applicable ATC within 24 hours of all details concerning any reported arrest.

32.5 Duty to Provide Security Data

The Contractor will maintain the security of State of Florida Data including, but not limited to, a secure area around any display of such Data or Data that is otherwise visible. The Contractor will also comply with all state and federal rules and regulations regarding security of information, including HIPPA when applicable. Data cannot be disclosed to any person or entity that is not directly approved to participate in the SOW set forth in any resulting ATC or PO.

The Contractor must deliver an attestation describing the classification of Customer data consumed by the Solution to ensure suitable controls are considered for classified data. Additionally, the Contractor will provide documentation and evidence describing the technical security controls commensurate with the data's classification as defined in Chapter 60GG-2, F.A.C. For any data identified as uniquely valuable to the Customer, the Contractor must provide a disaster recovery plan which must be approved by the Customer.

32.6 Screening Compliance Audits and Security Inspections

The Purchaser reserves the right to audit the Contractor's background screening process upon two (2) business days prior written notice to the Contractor during the Term of the PO and any applicable ATC. In the event of an incident as defined in section 282.0041, F.S., the Department will have the right to inspect to meet all applicable state and federal rules and regulations upon two (2) business days prior written notice to the Contractor to ensure that access to the State of Florida Data is secure and in compliance with any PO or applicable ATC.

32.7 Record Retention

The Customer will maintain ownership of all data consumed by the Solution. For all such data, Contractor shall comply with and grant all rights in Section 18.2 to each Customer.

The Contractor shall retain a list of all persons with Access to Data, including a statement confirming that each person has passed the background screening required herein. Such a statement shall not include the substance of the screening results, only that the person has passed the screening.

The Contractor shall create a written policy for the protection of Data, including a policy and procedure for Access to Data. The Contractor shall document and record, with respect to each instance of Access to Data:

- 1) The identity of all individual(s) who accessed data in any way, whether those individuals are authorized persons or not.
- 2) The duration of the individual(s)' access to Data, including the time and date at which the access began and ended.
- 3) The identity, form, and extent of Data accessed, including, but not limited to, whether the individual accessed partial or redacted versions of Data, read-only versions of Data, or editable versions of Data.
- 4) The nature of the access to Data, including whether Data was edited or shared with any other individual or entity during the duration of the access, and, if so, the identity of the individual or entity.

The Contractor shall retain the written policy and information required in this section for the duration of the Contract and a period of no less than five (5) years from the date of termination of the Contract and any Contract extensions. The written policy and information required in this section shall be included in Department's or the Purchaser's audit and screening abilities as defined in Section 30.6, Screening Compliance Audits and Security Inspections. The written policy and information required in this section shall also be subject to immediate disclosure upon written or

oral demand at any time by the Department, the Purchaser, or its designated agents or auditors.

Failure to compile, retain, and disclose the written policy and information as required in this section shall be considered a breach of any ATC(s) and PO(s). The resulting damages to the Department from a breach of this section are by their nature impossible to ascertain presently and will be difficult to ascertain in the future. The issues involved in determining such damages will be numerous, complex, and unreasonably burdensome to prove. The Contractor, the Customer, and the Department acknowledge that these financial consequences are liquidated damages, exclusive of any other right to damages, not intended to be a penalty and solely intended to compensate for unknown and unascertainable damages. The Contractor therefore agrees to credit the affected Customer, the sum of **\$500.00** for each breach of this section.

32.8 Indemnification

The Contractor agrees to defend, indemnify, and hold harmless the Department and any applicable Customers, the State of Florida, its officers, directors and employees for any claims, suits or proceedings related to a breach of this section. The Contractor will include credit monitoring services at its own cost for those individuals affected or potentially affected by a breach of this section for a two-year period following the breach.

33.0 LOCATION OF DATA

In accordance with Rule 60GG-4.002, F.A.C., the Contractor, including its employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees, or other persons operating under their direction, are prohibited from (i) performing any of the services under any applicable ATC or PO outside of the continental United States, or (ii) sending, transmitting, storing, or accessing any State of Florida data, outside of the continental United States. The Parties agree that a violation of this provision will:

- a) Result in immediate and irreparable harm to the Purchaser, the Department, or the Customer, entitling the Purchaser, the Department, or the Customer to immediate injunctive relief, provided, however, this shall not constitute an admission by the Contractor to any liability for damages under subsection (c) below or any claims, liability, or damages to a third party, and is without prejudice to the Contractor in defending such claims.
- b) Entitle the Purchaser, the Department, or the Customer, as applicable, to a credit or payment, at the Purchaser's discretion, of \$50,000 per violation, with a cumulative total cap of \$500,000 per event. This credit or payment is intended only to cover the Purchaser's, the Department's, or the Customer's internal staffing and administrative costs of investigations and audits of the transmittal of State of Florida data outside the U.S.
- c) Entitle the Purchaser, the Department, or the Customer, as applicable, to recover damages, if any, arising from a breach of this subsection and beyond those covered under subsection b).

The credits or payments in subsection b) are a reasonable approximation of the internal costs for investigations and audits from a violation. The credits or payments are in the nature of liquidated damages and not intended to be a penalty. By executing any resulting ATC or performing under any resulting PO, the Contractor acknowledges and agrees the costs

intended to be covered by subsection b) are not readily ascertainable and will be difficult to prove. The Contractor agrees that it will not argue, and is estopped from arguing, that such costs are a penalty or otherwise unenforceable. For purposes of determining the amount of costs due hereunder, a group of violations relating to a common set of operative facts (e.g., same location, same time period, same off-shore entity) shall be treated as a single violation. The costs will be applied as a financial consequence and are exclusive of any other right to damages.

34.0 DATA TRANSMISSION

Solution data shall only be transmitted through secure transmission methods utilizing a National Institute of Standards and Technology approved means of electronic encryption as well as password protection and in a file format and layout determined by the Department or the Purchaser, as applicable. Solution data shall not be transmitted via any other means, including electronic mail. If applicable to any transmission of the Solution data, both transmitter and the receiver shall completely and permanently remove Solution data from any temporary transfer location within twenty-four (24) hours of receipt of the Solution data.

35.0 TERMS AND CONDITIONS

The Department shall not accept any unrequested terms or conditions submitted by a vendor, including any appearing in documents attached as part of the vendor's Quote or on documents submitted after award. In submitting its Quote, the vendor agrees that any additional terms or conditions, whether submitted intentionally or inadvertently, shall have no force or effect, though items that the Department identified herein as negotiable may be negotiated. The Department will not accept or comply with any automatic renewal language within the vendor's Quote or any associated document. Any automatic renewal language will be deemed null and void. All licenses purchased through this RFQ shall have a one-year term, which may only be renewed by the Department through a new purchase order. The aforementioned provision is non-negotiable.

36.0 COOPERATIVE PURCHASING

Pursuant to their own governing laws, and subject to the agreement of the Contractor, Customers may make purchases in accordance with the terms and conditions contained herein. The Department shall not be a party to any transaction between the Contractor and any other Purchaser.

37.0 PRICE ADJUSTMENTS

The Contractor shall apply to the Department and Purchaser any price decrease effectuated during the Contract term by reason of market change or special sales offered to other customers. Such a price decrease applies regardless of whether any related equipment is rented or leased by the Department or Purchaser under the Contract. Price increases are rejected, unless otherwise stated. All prices are firm and shall be held for the duration of the Contract term.

38.0 FINANCIAL STABILITY

The Contractor is required to have financial stability in accordance with section 287.057 (27)(b), F.S. The Department will not entertain terms and condition negotiations with third parties regarding financing or funding associated with this RFQ.

39.0 RFQ ATTACHMENTS

Attachment A, Price Sheet
Attachment B, Contact Information Sheet

Agency Term Contract (Redlines or modifications to the ATC are not permitted.)
Department's Purchase Order Terms and Conditions
Non-Disclosure Agreement (Redlines or modifications to the NDA are not permitted.)

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT A PRICE SHEET

I. Alternate Contract Source (ACS)

Check the ACS contract the Quote is being submitted in accordance with:

- _____ 43210000-US-16-ACS Technology Products, Services, Solutions, and Related Products and Services
- _____ 43230000-NASPO-16-ACS Cloud Solutions
- _____ 43230000-23-NASPO-ACS Software Value Added Reseller (SVAR)

II. Pricing Instructions

The vendor shall provide fixed rates quoted at or below the rates in the applicable ACS contract selected in Section I above. FL[DS] anticipates purchasing the endpoint detection and response Solution for FL[DS] and all Customers. No matter the quantity, the vendor may not exceed the quoted unit price. The Department reserves the right to utilize the quoted unit pricing during the term of any applicable ATC and PO. Prices are ceiling rates inclusive of any and all costs associated with providing services.

III. Pricing

Initial Term Pricing (Years 1-3)		
Item No.	Description	Rate Per Device
1	<p><u>Initial Software Year</u> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	\$ _____
2	<p><u>Subsequent Software Year</u> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ _____

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	SKU Description	Market Price	ACS Price

V. Waterfall Pricing (Optional)

The Department is seeking an optional waterfall pricing model which leverages volume discounts. Vendors are encouraged to provide a pricing structure which specifies a volume range at which larger discounts could be applied. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

VI. State of Florida Enterprise Pricing (Optional)

The Department is also seeking an optional annual fixed rate to provide the Solution and services to all potential FL[DS] Customers. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

VII. Value-Added Services (Optional)

If vendors are able to offer additional services and/or commodities for endpoint detection and response, at no additional cost to the Department, the vendor may offer the Department value-added services, in addition to the services and/or commodities expressly sought by this RFQ.

Per **Section 31.0**, Scrutinized Companies, a vendor submitting a Quote must certify that their company is not participating in a boycott of Israel. By signing below, the vendor so certifies. Additionally, the person submitting the quote and pricing is authorized to respond to this RFQ on the vendor's behalf, as confirmed by the signature below.

Vendor Name

Signature

FEIN

Signatory Printed Name

Date

**ATTACHMENT B
CONTACT INFORMATION SHEET**

I. Contact Instructions

The vendor shall provide the contact information for the Quote and a contact for the resulting ATC and PO contact in the table below.

II. Contact Information

	Contact for Quoting Purposes	Contact for the ATC and PO (if awarded)
Name:		
Title:		
Address (Line 1):		
Address (Line 2):		
City, State, Zip Code		
Telephone (Office):		
Telephone (Mobile):		
Email:		

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Section 1. Purchase Order.

A. Composition and Priority.

The Contractor agrees to provide commodities or contractual services to the Agency within the manner and at the location specified in the Purchase Order, and any attachments to the Purchase Order. These Purchase Order Terms and Conditions, whether generic or specific, shall take precedence over any inconsistent or conflicting provision in the State of Florida, General Contract Conditions, PUR 1000. Additionally, the terms of the Purchase Order supersede the terms of any and all prior agreements with respect to this purchase.

B. Initial Term.

Unless otherwise specified, the Purchase Order begins on the date of issuance. Contractual services or commodities to be provided by the Contractor shall be completed by the date specified on the Purchase Order end date.

Section 2. Performance.

A. Performance Standards.

The Contractor agrees to perform all tasks and provide deliverables as set forth in the Statement of Work and attachments to the Purchase Order. The Agency shall be entitled at all times, upon request, to be advised as to the status of work being done by the Contractor and of the details thereof. Coordination shall be maintained by the Contractor with representatives of the Agency, or of other agencies involved in the project on behalf of the Agency.

B. Performance Deficiency.

If the Agency determines that the performance of the Contractor is unsatisfactory, the Agency may notify the Contractor of the deficiency to be corrected, which correction shall be made within a time-frame specified by the Agency. The Contractor shall provide the Agency with a corrective action plan describing how the Contractor will address all issues of contract non-performance, unacceptable performance, and failure to meet the minimum performance levels, deliverable deficiencies, or contract non-compliance. If the corrective action plan is unacceptable to the Agency, the Contractor will be assessed a non-performance retainage equivalent to 10% of the total invoice amount or as specified in the contractual documents. The retainage will be applied to the invoice for the then-current billing period. The retainage will be withheld until the Contractor resolves the deficiency. If the deficiency is subsequently resolved, the Contractor may invoice the Agency for the retained amount during the next billing period. If the Contractor is unable to resolve the deficiency, the funds retained will be forfeited.

Section 3. Payment and Fees.

A. Payment Invoicing.

The Contractor will be paid upon submission of properly certified invoice(s) to the Agency after delivery and acceptance of commodities or contractual services is

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

confirmed in writing by the Agency. Invoices shall contain detail sufficient for audit thereof and shall contain the Purchase Order and the Contractor's Federal Employer Identification Number or Social Security Number.

B. Payment Timeframe.

Section 215.422, Florida Statutes (F.S.), provides that agencies have five (5) working days to inspect and approve commodities or contractual services. Items may be tested for compliance with specifications. Items delivered not conforming to specifications may be rejected and returned at the Contractor's expense. Interest penalties for late payment are also provided for in section 215.422, F.S. A Vendor Ombudsman, whose duties include acting as an advocate for Vendors who may be experiencing problems obtaining timely payment(s) from an Agency, may be contacted at 850-413-5516, or Vendors may call the State Comptroller's Hotline at 1-800-848-3792.

C. MyFloridaMarketPlace Fees.

The following language is included pursuant to rule 60A-1.031, Florida Administrative Code:

The State of Florida, through the Department of Management Services, has instituted MyFloridaMarketPlace, a statewide eProcurement system pursuant to section 287.057(22), Florida Statutes. Payments issued by Agencies or Eligible Users to Vendors for purchases of commodities or contractual services are subject to Transaction Fees, as prescribed by rule 60A-1.031, Florida Administrative Code, or as may otherwise be established by law. Vendors shall submit monthly reports required by the rule. All reports shall be subject to audit. Failure to pay Transaction Fees or submit reports shall constitute grounds for default and exclusion from business with the State of Florida.

D. Payment Audit.

Records of costs incurred under terms of the Purchase Order shall be maintained and made available to the Agency upon request at all times during the period of the Purchase Order, and for a period of three years thereafter. Records of costs incurred shall include the Contractor's general accounting records, together with supporting documents and records of the Contractor and all subcontractors performing work, and all other records of the Contractor and subcontractors considered necessary by the Agency for audit.

E. Annual Appropriation and Travel.

Pursuant to section 287.0582, F.S., if the Purchase Order binds the State or an executive agency for the purchase of services or tangible personal property for a period in excess of one (1) fiscal year, the State of Florida's performance and obligation to pay under this contract is contingent upon an annual appropriation by the Legislature. Travel expenses are not reimbursable unless specifically authorized in writing, and shall be reimbursed only in accordance with section 112.061, F.S.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Section 4. Liability.

A. Indemnity.

To the extent permitted by Florida law, the Contractor agrees to indemnify, defend, and hold the State of Florida, its officers, employees and agents harmless from all fines, claims, assessments, suits, judgments, or damages, consequential or otherwise, including court costs and attorney's fees, arising out of any acts, actions, breaches, neglect or omissions of the Contractor, its employees, agents, subcontractors, assignees or delegates related to the Purchase Order, as well as for any determination arising out of or related to the Purchase Order, that the Contractor or Contractor's employees, agents, subcontractors, assignees or delegates are not independent contractors in relation to the Agency. The Purchase Order does not constitute a waiver of sovereign immunity or consent by the Agency or the State of Florida or its subdivisions to suit by third parties.

B. Payment for Claims.

The Contractor guarantees the payment of all just claims for materials, supplies, tools, or labor and other just claims against the Contractor or any employee, agent, subcontractor, assignee or delegate in connection with the Purchase Order.

C. Liability Insurance.

The Contractor shall maintain insurance sufficient to adequately protect the Agency from any and all liability and property damage/hazards which may result from the performance of the Purchase Order. All insurance shall be with insurers qualified and duly licensed to transact business in the State of Florida. If required by the Agency and prior to commencing any work the Contractor shall provide Certification(s) of Insurance evidencing that all appropriate coverage is in full force and showing the Agency to be an additional insured.

D. Workers' Compensation.

The Contractor shall maintain Workers' Compensation insurance as required under the Florida Workers' Compensation Law.

E. Performance Bond.

Unless otherwise prohibited by law, the Agency may require the Contractor to furnish, without additional cost to the Agency, a performance bond or irrevocable letter of credit or other form of security for the satisfactory performance of work hereunder. The Agency shall determine the type and amount of security.

Section 5. Compliance with Laws.

A. Conduct of Business.

The Contractor shall comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and authority. For example, the Contractor shall comply with Section 247A of the Immigration and Nationality Act, the

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Americans with Disabilities Act, Health Insurance Portability and Accountability Act, and all prohibitions against discrimination on the basis of race, religion, sex, creed, national origin, handicap, marital status, or veteran's status.

Pursuant to subsection 287.058(1), F.S., the provisions of subparagraphs 287.058(1)(a)-(c), and (g), F.S., are hereby incorporated by reference, to the extent applicable.

B. Lobbying.

In accordance with sections 11.062 and 216.347, F.S., the Purchase Order funds are not for the purpose of lobbying the Legislature, the judicial branch, or an Agency. Pursuant to subsection 287.058(6), F.S., the Purchase Order does not prohibit the Contractor from lobbying the executive or legislative branch concerning the scope of services, performance, term, or compensation regarding the Purchase Order, after the Purchase Order's execution and during the Purchase Order's term.

C. Gratuities.

The Contractor shall not, in connection with this or any other agreement with the State, directly or indirectly (1) offer, give, or agree to give anything of value to anyone as consideration for any State officer or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty, or (2) offer, give, or agree to give to anyone anything of value for the benefit of, or at the direction or request of, any State officer or employee.

D. Cooperation with Inspector General.

Pursuant to subsection 20.055(5), F.S., Contractor, and any subcontractor to the Contractor, understand and will comply with their duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing. Upon request of the Inspector General or any other authorized State official, the Contractor shall provide any type of information the Inspector General deems relevant to the Contractor's integrity or responsibility. Such information may include, but shall not be limited to, the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Purchase Order. The Contractor shall retain such records for three (3) years after the expiration of the Purchase Order, or the period required by the General Records Schedules maintained by the Florida Department of State (available at: <http://dos.myflorida.com/library-archives/records-management/general-records-schedules/>), whichever is longer. The Contractor agrees to reimburse the State for the reasonable costs of investigation incurred by the Inspector General or other authorized State official for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the State which results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to: salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees.

E. Public Records.

To the extent required by the Florida Public Records Act, Chapter 119, F.S., the Contractor shall maintain and allow access to public records made or received in

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

conjunction with the Purchase Order. The Purchase Order may be terminated for cause by the Agency for the Contractor's refusal to allow access to public records.

F. Communications and Confidentiality.

The Contractor agrees that it shall make no statements, press releases, or publicity releases concerning the Purchase Order or its subject matter or otherwise disclose or permit to be disclosed any of the data or other information obtained or furnished in compliance with the Purchase Order, or any particulars thereof, during the period of the Purchase Order, without first notifying the Agency's Contract Manager or the Agency's designated contact person and securing prior written consent. The Contractor shall maintain confidentiality of all confidential data, files, and records related to the services and/or commodities provided pursuant to the Purchase Order and shall comply with all state and federal laws, including, but not limited to sections 381.004, 384.29, 392.65, and 456.057, F.S. The Contractor's confidentiality procedures shall be consistent with the most recent version of the Agency's security policies, protocols, and procedures. The Contractor shall also comply with any applicable professional standards with respect to confidentiality of information.

G. Intellectual Property.

Unless specifically addressed in the Purchase Order, intellectual property rights to all property created or otherwise developed by the Contractor for the Agency will be owned by the State of Florida through the Agency at the completion of the Purchase Order. Proceeds to any Agency derived from the sale, licensing, marketing or other authorization related to any such Agency-controlled intellectual property right shall be handled in the manner specified by applicable state statute.

H. Convicted and Discriminatory Vendor Lists.

In accordance with sections 287.133 and 287.134, F.S., an entity or affiliate who is on the Convicted Vendor List or the Discriminatory Vendor List may not perform work as a contractor, supplier, subcontractor, or consultant under the Purchase Order with any Agency.

Section 6. Termination.

A. Termination for Convenience.

The Purchase Order may be terminated by the Agency in whole or in part at any time in the best interest of the Agency. If the Purchase Order is terminated before performance is completed, the Contractor shall be paid only for that work satisfactorily performed for which costs can be substantiated. Such payment, however, may not exceed an amount which is the same percentage of the Purchase Order price as the amount of work satisfactorily performed. All work in progress shall become the property of the Agency and shall be turned over promptly by the Contractor.

B. Termination for Cause.

If the Agency determines that the performance of the Contractor is not satisfactory, the Agency shall have the option of (a) immediately terminating the Purchase Order, or (b)

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

notifying the Contractor of the deficiency with a requirement that the deficiency be corrected within a specified time, otherwise the Purchase Order will be terminated at the end of such time, or (c) take other action deemed appropriate by the Agency.

Section 7. Subcontractors and Assignments.

A. Subcontractors.

The Contractor shall not subcontract any work under the Purchase Order without the prior written consent of the Agency. The Contractor is fully responsible for satisfactory completion of all subcontracted work.

B. Assignment.

The Contractor shall not sell, assign or transfer any of its rights, duties or obligations under the Purchase Order without the prior written consent of the Agency. In the event of any assignment, the Contractor remains secondarily liable for performance of the Purchase Order, unless the Agency expressly waives such secondary liability. The Agency may assign the Purchase Order with prior written notice to the Contractor.

Section 8. RESPECT and PRIDE.

A. RESPECT.

In accordance with subsection 413.036(3), F.S., if a product or service required for the performance of the Purchase Order is on the procurement list established pursuant to subsection 413.035(2), F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES THAT ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM A NONPROFIT AGENCY FOR THE BLIND OR FOR THE SEVERELY HANDICAPPED THAT IS QUALIFIED PURSUANT TO CHAPTER 413, FLORIDA STATUTES, IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 413.036(1) AND (2), FLORIDA STATUTES; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THE STATE AGENCY INsofar AS DEALINGS WITH SUCH QUALIFIED NONPROFIT AGENCY ARE CONCERNED.

Additional information about the designated nonprofit agency and the products it offers is available at <http://www.respectofflorida.org>.

B. PRIDE.

In accordance with subsection 946.515(6), F.S., if a product or service required for the performance of the Purchase Order is certified by or is available from Prison Rehabilitative Industries and Diversified Enterprises, Inc. (PRIDE) and has been approved in accordance with subsection 946.515(2), F.S., the following statement applies:

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES WHICH ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM THE CORPORATION IDENTIFIED UNDER CHAPTER 946, F.S., IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 946.515(2) AND (4), F.S.; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THIS AGENCY INsofar AS DEALINGS WITH SUCH CORPORATION ARE CONCERNED.

Additional information about PRIDE and the products it offers is available at <http://www.pride-enterprises.org>.

Section 9. Miscellaneous.

A. Independent Contractor.

The Contractor and its employees, agents, representatives, and subcontractors are not employees or agents of the Agency and are not entitled to the benefits of State of Florida employees. The Agency shall not be bound by any acts or conduct of the Contractor or its employees, agents, representatives, or subcontractors. The Contractor agrees to include this provision in all of its subcontracts under the Purchase Order.

B. Governing Law and Venue.

The laws of the State of Florida shall govern the Purchase Order. The Parties submit to the jurisdiction of the courts of the State of Florida exclusively for any legal action related to the Purchase Order. Further, the Contractor hereby waives any and all privileges and rights relating to venue it may have under Chapter 47, F.S., and any and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to those based on convenience. The Contractor hereby submits to venue in the county chosen by the Agency.

C. Waiver.

The delay or failure by the Agency to exercise or enforce any of its rights under the Purchase Order shall not constitute waiver of such rights.

D. Modification and Severability.

The Purchase Order may only be modified by a change order agreed to by the Agency and the Contractor. Should a court determine any provision of the Purchase Order is invalid, the remaining provisions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the Purchase Order did not contain the provision held to be invalid.

E. Time is of the Essence.

Time is of the essence with regard to each and every obligation of the Contractor. Each such obligation is deemed material, and a breach of any such obligation (including a breach resulting from untimely performance) is a material breach.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

F. Background Check.

The Agency may require the Contractor and its employees, agents, representatives and subcontractors to provide fingerprints and be subject to such background check as directed by the Agency. The cost of the background check(s) shall be borne by the Contractor. The Agency may require the Contractor to exclude the Contractor's employees, agents, representatives or subcontractors based on the background check results.

G. E-Verify.

In accordance with Executive Order 11-116, the Contractor agrees to utilize the U.S. Agency of Homeland Security's E-Verify system, <https://e-verify.uscis.gov/emp>, to verify the employment eligibility of all new employees hired during the term of the Purchase Order for the services specified in the Purchase Order. The Contractor shall also include a requirement in subcontracts that the subcontractor shall utilize the E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor during the Purchase Order term.

H. Commodities Logistics.

The following provisions shall apply to all Purchase Orders unless otherwise indicated in the contract documents:

- 1) All purchases are F.O.B. destination, transportation charges prepaid.
- 2) Each shipment must be shipped to the address indicated on the face of the Purchase Order and marked to the attention of the individual identified, if any. Each shipment must be labeled plainly with the Purchase Order number and must show the gross, tare, and net weight. A complete packing list must accompany each shipment. This paragraph shall also apply to any third party who ships items on behalf of the Contractor.
- 3) No extra charges shall be applied for boxing, crating, packing, or insurance.
- 4) The following delivery schedule shall apply: 8:00 AM – 4:00 PM, Monday through Friday, excluding legal holidays.
- 5) If delivery to the specified destination cannot be made on or before the specified date, notify the Agency immediately using the contact information provided in the MyFloridaMarketPlace system.
- 6) The Agency assumes no liability for merchandise shipped to other than the specified destination.
- 7) Items received in excess of quantities specified may, at Agency's option, be returned at the Contractor's expense. Substitutions are not permitted.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK



4050 Esplanade Way
Tallahassee, FL 32399-0950

Ron DeSantis, Governor
Pedro Allende, Secretary

**CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT
BETWEEN
FLORIDA DEPARTMENT OF MANAGEMENT SERVICES
AND**

This Confidentiality and Non-Disclosure Agreement (“Agreement”) is between the Florida Department of Management Services (“Department”), a state agency, and (“Recipient”), referred to herein collectively as the “Parties” and individually as a “Party.”

WHEREAS, Recipient has or will enter into a Purchase Order or Agency Term Contract under Request for Quote No. DMS-22/23-155, Endpoint Detection and Response Solution (“Solution”);

WHEREAS, in furtherance of providing these services and/or commodities, Recipient may access, receive, or create Confidential Information from the Department or any third-party beneficiaries; and

WHEREAS, the Department maintains certain protections on such Confidential Information and desires to set forth the terms Recipient is required to adhere to.

NOW THEREFORE, for the mutual and valuable consideration acknowledged by both Parties, the Parties agree as follows:

1. Definitions.

- (a) **Access**: Means the ability or authorization to create, inspect, transmit, approach, instruct, communicate with, store, retrieve, or otherwise make use of any Confidential Information, regardless of type, form, or nature of storage. “Access” to a computer system or network includes local and remote access.
- (b) **Affiliates**: Any agents, affiliates, partners, subcontractors, resellers, distributors, dealers, or other entities associated with Recipient that have Access to the Confidential Data.
- (c) **Agreement-related Materials**: Materials created or provided by Recipient while performing the Agreement.
- (d) **Confidential Information**: Information that is restricted from public disclosure based on federal or State laws and regulations including, but not limited to, those related to privacy, confidentiality, security, personally identifying information, personal health, business or trade secret information, and other information exempt from state public records law. “Confidential Information” includes information disclosed, orally or otherwise, before, on, or after this Agreement effective date by the Department to Recipient, and whether or not marked, designated, or otherwise identified as “confidential.” Any information derived from Confidential Information and/or created by Recipient pursuant to this Agreement which must be restricted from public disclosure based on federal or State laws and regulations shall be considered Confidential Information subject to the restrictions set forth in this Agreement.

Specifically, Recipient will receive and may create or learn of information which include network schematics, hardware and software configurations, or encryption, or which identify detection, investigation, or response practices for suspected or confirmed IT security incidents, including suspected or confirmed breaches, the disclosure of which would facilitate unauthorized access, modification, disclosure, or destruction of information, IT resources, or information relating security, which are confidential and exempt from public disclosure pursuant to section 282.318(5), Florida Statutes (F.S.).

- (e) Customer: Agencies as defined in section 287.012, Florida Statute (F.S.), and Eligible Users as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.).
- (f) State: The State of Florida.

2. **Term and Termination.** This Agreement is effective upon signature by both Parties. This Agreement may be terminated by the Department when determined to be in the best interest of the State of Florida by providing Recipient with advance written notice.
3. **Intended Third Party Beneficiary.** Customers receiving services under the Solution are intended third party beneficiaries of this Agreement, entitled to enforce any rights hereunder for their benefit.
4. **Confidential Information Use.** Use of the Confidential Information shall be limited to the provisions set forth herein and to the extent necessary to provide the services and/or commodities. The Department retains full rights and title to all Confidential Information provided by it, and any information derived therefrom. Recipient has no ownership rights to the Confidential Information provided under this Agreement, or any information derived therefrom.
5. **Recipient Obligations.** Recipient shall: 1) maintain the confidentiality of all the Confidential Information pursuant to this Agreement, as required herein, 2) comply with all federal and State laws and regulations related to information privacy and security, and 3) ensure that any Affiliates comply with the preceding two requirements as to any Confidential Information shared with or otherwise Accessed by the Affiliate. Recipient shall take all measures necessary to protect against improper Access to and/or disclosure or theft of the Confidential Information and will ensure only those individuals performing services contemplated in this Agreement will be permitted to Access the Confidential Information. Recipient shall perform the following measures to preserve the privacy, security, confidentiality, integrity, and accessibility of the Confidential Information which includes, but is not limited to:
 - (a) Using the Confidential Information only to provide services and/or commodities as contemplated in this Agreement and not otherwise using the Confidential Information for Recipient's own benefit or the benefit of others, or in violation of any applicable laws or regulations;
 - (b) Not creating derivative works based upon the Confidential Information, copying the Confidential Information, or publishing or disclosing the Confidential Information to any individual or entity except in accordance with this Agreement;
 - (c) Implementing and maintaining protective administrative, technical, and organizational security measures appropriate to the nature of the Confidential Information to safeguard against unauthorized Access, disclosure, or theft of the Confidential Information;
 - (d) Maintaining the confidentiality of the Confidential Information under this Agreement in accordance with Department policies and procedures and applicable State and federal laws and regulations;

- (e) Storing and safeguarding the Confidential Information in a physically and electronically secure location where Access is limited to authorized persons;
- (f) Maintaining an up-to-date list of individuals who are authorized to Access the Confidential Information;
- (g) Instructing and requiring all individuals authorized to Access the Confidential Information to adhere to the confidentiality requirements set forth in this Agreement prior to being granted Access to the Confidential Information;
- (h) Not allowing, through action or inaction, any Confidential Information to be sent by any medium, transmitted, or to be Accessed outside of the United States. For the purposes of this restriction, "Access" does not include remote support sessions for devices that might contain the Confidential Information; however, during the remote support session the Department requires Recipient to escort the remote support access and maintain visibility of the actions taken during the remote support access. Requests for remote access will be submitted to the Department's Contract Manager. With approval, third parties may be granted time-limited terminal service access to information technology resources as necessary for fulfillment of related responsibilities. Remote connections are subject to detailed monitoring via two-way log reviews and the use of other tools; and
- (i) Performing all actions necessary to assist with all tasks in furtherance of the Department's efforts to comply with the obligations under Chapters 60FF and 60GG, Florida Administrative Code, as applicable.

6. Liability. By signing this Agreement, Recipient acknowledges Recipient shall be responsible and liable for the acts and omissions of any of Recipient's employees and/or the Affiliate(s) that result in a violation of this Agreement as if such acts or omissions were Recipient's acts or omissions. Recipient represents that it will enter into a written agreement with an Affiliate with Access to Confidential Information wherein it shall require the Affiliate agree to be bound by and adhere to the terms of this Agreement.

7. Notice of Breach. Recipient must notify the Department as expeditiously as practicable, but in all instances no later than within one (1) business day, in the event Recipient discovers any incident that involves, or which Recipient reasonably believes may involve, a breach of the Confidential Information which includes any unauthorized Access to or disclosure of the Confidential Information and/or which compromises the security, integrity, or confidentiality of the Confidential Information. Additionally, if the Department or Customer shares with Recipient information that is covered by section 501.171, F.S., Recipient is responsible for fulfilling all applicable requirements of section 501.171, F.S., including those that would otherwise be the responsibility of the Department or Customer. Recipient agrees to provide the Department and applicable Customers with all details associated with all breaches or suspected breaches and to work with the Department or the applicable Customer to investigate and resolve any breach, implement any necessary remedial measures, and perform all tasks to ensure full compliance with section 501.171, F.S., including, where applicable, providing any breach notifications to comply with this statutory requirement.

8. Indemnification. Recipient shall defend, indemnify, and hold harmless the Department, the Customer, and the State against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, in connection with any third-party claim, suit, action, or proceeding arising out of or resulting from a violation of any obligation set forth in this Agreement by Recipient (including its employees) or its Affiliates. The Agreement does not constitute a waiver of sovereign immunity or consent by the Department, Customers, or the State or its subdivisions to suit by third parties. The obligations of this paragraph shall survive the Agreement.

- 9. Contractual Remedies.** Recipient acknowledges that a breach of this Agreement, including disclosure of any of the Confidential Information, will cause irreparable injury to the Department or the Customer and will entitle the Department or the Customer, if applicable, to liquidated damages commensurate with the Department's or the Customer's internal staffing and administrative costs associated with addressing the breach. This will not preclude the Department or the Customer from recovering other damages it may suffer as a result of such a violation or seeking other legal remedies that may be available during or after the Agreement term, including obtaining injunctive relief against the breach or threatened breach of these Agreement terms.
- 10. Data Destruction.** Prior to the termination of this Agreement, Recipient shall assist the Department or the applicable Customer in exporting and extracting or destroying, at the Department's or the applicable Customer's direction, all information obtained from the Department or the applicable Customer by Recipient or created for the Department or the applicable Customer by Recipient pursuant to this Agreement at no cost, in a format acceptable to the Department or the applicable Customer without the need to purchase additional services and/or commodities. Additionally, when the Agreement is terminated, Recipient shall transfer to the Department, or the Customer as applicable, all such information in all its forms from the Department or the applicable Customer and shall destroy duplicate records in accordance with section 501.171(8), F.S., and, if applicable, section 119.0701, F.S. This obligation to transfer and destroy information survives the term of this Agreement.

Recipient shall adhere to established information destruction standards, such as those established by the National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization" (2014), in destroying duplicate information provided by the Department or the applicable Customer. See <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>. Recipient shall provide the Department, or the Customer as applicable, with written confirmation of destruction of Confidential Information in accordance with these standards. If Recipient is permitted by the Department or the applicable Customer to keep Confidential Information upon termination of this Agreement, Recipient shall continue to protect and maintain the confidentiality of the Confidential Information in accordance with applicable State and federal laws, rules, and regulations and such obligations set forth herein shall survive this Agreement.

- 11. Severability and Waiver.** If a court of competent jurisdiction deems any term or condition of this Agreement void or unenforceable, the other provisions are severable to that void provision, and will remain in full force and effect. However, to the fullest extent permitted by law, this Agreement shall be construed as if the scope or duration of such provision had been more narrowly drafted so as not to be invalid or unenforceable.

The delay or failure by the Department or the Customer to exercise or enforce any of its rights under this Agreement shall not constitute a waiver of such rights.

- 12. Governing Law and Venue.** The laws of the State of Florida govern the Agreement. The Parties submit to the jurisdiction of the courts of the State exclusively for any legal action related to the Agreement which arises during or after the Agreement term. Further, Recipient hereby waives all privileges and rights relating to venue it may have under Chapter 47, F.S., and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to, those based on convenience. Recipient hereby submits to venue in the county chosen by the Department or the applicable Customer.

13. Entire Agreement. This Agreement contains the entire understanding of the Parties regarding the matters set forth herein and shall supersede any prior negotiations or agreements, whether written or oral, with respect thereto.

IN WITNESS WHEREOF, the Parties agree to the terms and conditions of this Agreement and have duly authorized their respective representatives to sign it on the dates indicated below.

**FLORIDA DEPARTMENT
OF MANAGEMENT SERVICES**

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____



PROPOSAL RESPONSE

Florida Digital Service Endpoint Detection and Response Solution

Request for Quote (RFQ): DMS-22/23-155

Submit via Data Communications Products and Services
(43220000-NASPO-19-ACS)

Updated 6/14/2023



TABLE OF CONTENTS

1)	ENDPOINT DETECTION AND RESPONSE SOLUTION DOCUMENTATION.....	1
a)	Draft SLA	25
b)	Training & Support sla	25
c)	Implementation plan	25
	Cisco Secure Endpoint Initial Implementation.....	26
d)	MDR SLA (optional).....	26
e)	Future Integrations SLA (optional)	27
f)	Disaster Recovery Plan.....	27
2)	EXPERIENCE	33
	Industry Analyst and User Validation for Secure Endpoint	33
	Cisco Secure Endpoint Case Studies and Testimonials	34
	Case Studies.....	34
	Testimonials	35
3)	IMPLEMENTATION	37
4)	VALUE-ADDED SERVICES	38
5)	ATTACHMENT A – PRICE SHEET	41
6)	ATTACHMENT B – CONTACT INFORMATION SHEET	46
7)	NON-DISCLOSURE AGREEMENT	47

TABLE OF EXHIBITS

No table of figures entries found.

1) ENDPOINT DETECTION AND RESPONSE SOLUTION DOCUMENTATION

RFQ Text:

Documentation to describe the endpoint detection and response solution proposed and how it meets the requirements of this RFQ.

Response:

Presidio is proud to partner with Cisco in response to this RFQ. Cisco Secure Endpoint is a single-agent solution that provides comprehensive protection, detection, response, and user access coverage to defend against threats to your endpoints. Below is a detailed description of how Cisco Secure Endpoint meets the requirements as listed in the RFQ.

6.1. Software Solution/Specifications

The Solution shall detect and respond to threats on endpoint devices such as laptops, desktops, servers, and mobile devices. Endpoint Detection and Response (EDR) solutions typically use a combination of techniques such as behavioral analysis, machine learning, and threat intelligence to identify and respond to security incidents in real-time. The primary purpose of EDR is to detect and respond to advanced threats that have bypassed traditional security defenses such as firewalls and antivirus software. This is accomplished by collecting data from endpoint devices, analyzing it for signs of suspicious activity, and taking automated or manual actions to isolate and neutralize threats. EDR solutions can help organizations improve their overall security posture by providing visibility into the activities taking place on endpoint devices, helping security teams respond to incidents more quickly and effectively, and providing valuable information that can be used to improve security processes and policies.

RESPONSE:

Cisco Secure Endpoint excels in detecting and responding to threats on a variety of endpoint devices such as laptops, desktops, servers, and mobile devices, providing your organization with comprehensive coverage.

Threat Detection: Leveraging behavioral analysis, machine learning, dynamic analysis, sandboxing, and threat intelligence from Cisco Talos, Cisco Secure Endpoint actively monitors for suspicious activity, ensuring threats are identified in real time. It does this by analyzing a vast array of data from endpoints, such as file activity, network connections, and system processes.

Response to Advanced Threats: Cisco Secure Endpoint is designed to detect advanced threats that have bypassed traditional security defenses. Once a threat is detected, the solution can automatically respond based on predefined policies or manual input from security teams. The automated responses can include isolating affected endpoints, terminating malicious processes, and removing malicious files.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Real-Time Visibility: Cisco Secure Endpoint provides real-time visibility into all activities taking place on endpoint devices. This allows security teams to quickly detect and respond to security incidents and helps in identifying patterns of behavior that could indicate a broader security concern.

Improving Security Posture: By providing detailed information about threats and security incidents, Cisco Secure Endpoint helps organizations continuously improve their security processes and policies. This intelligence, combined with insights from Cisco Talos, ensures your organization stays ahead of evolving threats.

Integration: As part of the SecureX platform, Cisco Secure Endpoint can integrate with other security solutions, both from Cisco and third-party vendors. This enables your organization to have a coordinated, unified response to threats, further enhancing your security posture.

In summary, Cisco Secure Endpoint not only detects and responds to advanced threats on endpoint devices but also provides valuable insights to improve your organization's overall security posture.

6.1.1. Multi-Tenant

The Solution shall support a multi-tenant, multi-organization architecture. Each tenant must have its own instance and each instance must aggregate up to a single instance and view. The aggregated instance will support enterprise security operations. The Solution shall provide dashboards for single-source visibility into threats, investigations, and trends.

RESPONSE:

Cisco Secure Endpoint is built to support a multi-tenant, multi-organization architecture, ensuring that each tenant has its own instance while still allowing for data to aggregate up to a single view for investigations, which is invaluable for enterprise security operations.

Multi-Tenant Architecture: Cisco Secure Endpoint enables each tenant to have its own instance, ensuring complete data segregation and confidentiality. This design means each tenant can manage its own policies, configurations, and alerts independently.

Aggregated View: Despite the independence of each instance, Cisco Secure Endpoint also enables a unified, aggregated view across all tenants for investigations. This is particularly useful for enterprise security operations, as it provides a comprehensive perspective of the security posture across the entire organization, allowing for more effective threat detection and response.

Dashboards: Cisco Secure Endpoint comes with a powerful dashboard that provides single-source visibility into threats, investigations, and trends across all tenants. This unified view aids in identifying patterns and correlations that might not be visible when looking at each tenant individually. These dashboards are customizable and can include a variety of widgets to meet the specific needs of your organization.

This dashboard can be accessed via SecureX, Cisco's integrated security platform, which provides a centralized interface for managing and monitoring all of Cisco's security solutions. This allows your organization to have a streamlined security operations experience, minimizing the complexity often associated with managing multi-tenant environments.

In summary, Cisco Secure Endpoint provides robust support for multi-tenant, multi-organization architectures, delivering both the necessary isolation for individual tenants and the unified visibility required for effective enterprise security operations.

6.1.2. Scalability

The Solution shall provide the ability to scale to support a large number of tenants and their endpoints.

RESPONSE:

Cisco Secure Endpoint is designed with scalability as a core feature, ensuring it can accommodate the needs of an organization of any size, with any number of tenants and endpoints.

Scalability: Built on Cisco's robust cloud infrastructure, Cisco Secure Endpoint can scale dynamically to support a large number of tenants and their associated endpoints. Whether your organization is growing, merging, or acquiring, Cisco Secure Endpoint can easily adapt to the changing scale of your operations.

Endpoint Support: Cisco Secure Endpoint is designed to handle a vast number of endpoints across multiple tenants. The solution can provide consistent, real-time visibility, threat detection, and response capabilities regardless of the number of endpoints.

Performance: Despite the scale, Cisco Secure Endpoint maintains high performance levels, ensuring real-time threat detection and response capabilities are not compromised. The cloud-based architecture is designed to efficiently distribute workloads, ensuring system performance remains consistent as the number of tenants and endpoints increases.

Cloud Infrastructure: The use of cloud infrastructure also ensures that system updates, threat intelligence updates, and new feature rollouts can be deployed seamlessly, without affecting system performance or requiring downtime. This ensures that all tenants, regardless of size or number of endpoints, are always benefiting from the latest security capabilities.

Management: Through the SecureX platform, management of a large number of tenants and their endpoints remains streamlined and efficient. SecureX provides a single-pane-of-glass view into your organization's security posture, simplifying the complexity often associated with managing large-scale, multi-tenant environments.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO[®]

In summary, Cisco Secure Endpoint is designed to scale and adapt to your organization's needs, ensuring consistent, high-quality endpoint security regardless of the number of tenants or endpoints.

6.1.3. Cloud Management

The Solution shall be provided as software as a service via cloud-hosted infrastructure to keep current with the latest releases of management server and endpoint agent software. The Solution shall allow capacity extensibility in the cloud with minimal impact on agent or management infrastructure.

RESPONSE:

Cisco Secure Endpoint is delivered as a Software as a Service (SaaS) solution, utilizing a cloud-hosted infrastructure. This approach brings several advantages to your organization.

Latest Releases: As a SaaS solution, Cisco Secure Endpoint ensures that you always have the latest versions of both the management server and endpoint agent software. Updates, enhancements, and patches are automatically applied in the background, without the need for manual intervention or system downtime.

Cloud Infrastructure: The cloud-based nature of the service allows for capacity extensibility with minimal impact on the agent or management infrastructure. As your organization grows or your needs change, you can seamlessly scale your usage of Cisco Secure Endpoint. The cloud infrastructure can dynamically adapt to accommodate increased data, more endpoints, or additional tenants.

Agent Impact: Updates to the endpoint agent software are pushed out automatically and can be scheduled to occur during non-peak hours to minimize impact on system performance. The agent itself is designed to be lightweight and efficient, ensuring endpoint performance is not adversely affected.

Management Infrastructure: Changes to the scale of your usage or updates to the system do not impact the management infrastructure. The SecureX platform provides a single interface for managing all aspects of your security operations, regardless of the number of endpoints or the scale of data being processed.

Security: The SaaS model also means that you're benefiting from Cisco's robust security measures. Data is encrypted both in transit and at rest, and Cisco's data centers are designed to be highly secure and resilient.

In summary, Cisco Secure Endpoint as a SaaS solution ensures you're always up to date, can easily scale your usage, and can do so with minimal impact on the agent or management infrastructure.

6.1.4. Managed Security Services

The Solution shall deploy and maintain managed security services to support Purchasers and Customers, particularly the advanced administration requirement of endpoint detection and response tools and incident response capabilities.

RESPONSE:

Cisco Secure Managed Detection and Response (MDR) combines an elite team of researchers, investigators, and responders with threat intelligence, automation and response capabilities, and defined investigation and response playbooks supported by Cisco Talos threat research. Secure MDR can reduce the time to detect and respond from months to minutes. Secure MDR leverages Cisco's world-class integrated security architecture to advance security operations capabilities by delivering 24x7x365 threat detection and response – faster – with relevant, meaningful, and prioritized response actions.

Benefits:

- **A stronger security posture that protects against threats with expert teams of researchers, investigators, and responders who provide always-on monitoring and response.**
- **Advanced security operations that leverage Cisco threat intelligence and automation.**
- **Management and prioritization of alert volume across cloud, on-premises network, and endpoints with defined investigation and response playbooks.**
- **Powerful integrated security architecture that provides greater visibility.**
- **24x7x365 analysis, investigation, and response to improve mean time to detect and respond to security threats.**
- **Detection, analysis, investigation, and response with Secure MDR**

Elite researchers, investigators, and responders in our global Security Operations Centers (SOCs) are provided with near-real-time alerts occurring within your cloud, on-premises networks, and endpoints. We engage with you to advance your security operations capabilities by providing clarity on attacks and expert guidance on how to eliminate threats quickly and prevent breaches.

Secure MDR includes:

Detection using an integrated cloud security ecosystem that improves mean time to detect and contain security threats. The service delivers relevant, high-confidence, and consistent results using proven methodologies, unique intelligence, and an experienced team.

Analysis through the enrichment of alerts, including Talos threat intelligence. Secure MDR provides attacker attributes and tactics to analysts along with the critical context needed to prioritize the impact and urgency of a threat.

Investigation of identified threats utilizing defined investigation playbooks that provide added context. When malware, ransomware, botnet, bad actors, and other bad behavior occurs, we make data-driven decisions that establish relevant, meaningful, and prioritized response actions.

Response with Security Orchestration and Automated Response (SOAR) and case management to execute defined response playbooks to provide detailed threat analysis, including recommended response actions.

Cisco Talos Intelligence Group, the largest non-governmental threat intelligence research team in the world, provides integrated threat intelligence that protects Cisco Secure MDR security technologies.

Coordination with Cisco Talos Incident Response for breach and forensic investigations provides next-level capabilities when an alert becomes a breach. Our team of forensic investigators can leverage the Secure MDR data repository and tools to respond to an emergency faster.

A **customer portal** provides access to the supported Cisco Security technologies and offers a robust dashboard, ticketing, reporting, and case management interface, providing both operations and executive visibility to all activities.

6.1.5. Prevention

The Solution shall block malware pre-execution using the platform's anti-malware prevention program.

RESPONSE:

Cisco Secure Endpoint utilizes a comprehensive approach to preventing malware, employing advanced techniques to block threats before they can execute.

Anti-Malware Prevention Program: The anti-malware capabilities of Cisco Secure Endpoint are built on a combination of signature-based detection, behavioral analysis, and machine learning. This combination allows the system to identify and block known threats, as well as detect and prevent previously unseen malware based on its behavior or other characteristics.

Pre-Execution Blocking: The solution uses a proactive approach to prevent malware execution. Using machine learning and cloud-based analytics, Cisco Secure Endpoint can identify potentially malicious files before they have a chance to run, blocking them and preventing potential harm.

File Reputation Analysis: Every file is scrutinized against Cisco's extensive file reputation database. If a file is identified as malicious or suspicious, it is blocked from executing.

File Trajectory and Retrospection: Cisco Secure Endpoint also tracks file trajectory across all endpoints, enabling it to identify the origin and scope of a threat. It offers retrospective security capabilities, which means if a file's reputation changes from good to bad after execution, administrators can track its trajectory and take necessary actions.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Sandboxing: Suspicious files can be further analyzed in a secure sandbox environment. If a file exhibits malicious behavior within the sandbox, it's classified as a threat and will be blocked from executing on the endpoints.

Integration with SecureX: The capabilities of Cisco Secure Endpoint are further enhanced when integrated with SecureX, Cisco's security platform. This allows for coordinated threat response across your entire security infrastructure, ensuring threats are quickly identified and mitigated.

In summary, Cisco Secure Endpoint is designed to block malware before it can cause harm, using a combination of advanced detection techniques and a proactive approach to threat prevention.

6.1.6. Product Usability

The Solution shall provide easy to understand, user-friendly interfaces with intuitive designs to facilitate user engagement, and clear documentation and support resources which instruct on use of the Solution.

RESPONSE:

Cisco Secure Endpoint is designed with usability in mind, ensuring that its interfaces are user-friendly and intuitive to facilitate user engagement.

User-Friendly Interface: The solution provides a clean, intuitive interface that enables users to quickly understand and navigate the system. The dashboard provides a single-source visibility into threats, investigations, and trends, which can be customized to meet the specific needs of your organization.

Intuitive Design: The design of the interface simplifies complex security tasks. Common tasks and functions are easily accessible, and the system provides clear visualizations and real-time updates to help users understand the current security posture and ongoing activities.

Documentation and Support Resources: Cisco provides comprehensive documentation for Secure Endpoint, including user guides, tutorials, and FAQs. These resources provide clear instructions on how to use the solution, and are regularly updated to reflect new features and capabilities.

Online Community and Support: In addition to documentation, Cisco has an extensive online community where users can ask questions, share experiences, and learn from experts. Cisco's support team is also available 24/7 to assist with any issues or concerns via TAC support included in the price of the software.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Training: Cisco offers training resources to help users get up to speed with the solution. These resources include webinars, video tutorials, and more in-depth training courses.

SecureX Integration: When integrated with SecureX, Cisco's security platform, users gain a centralized interface for managing and monitoring all of Cisco's security solutions. This simplifies the user experience and ensures a consistent, easy-to-understand interface across all security operations.

In summary, Cisco Secure Endpoint is designed to be easy to use, with clear documentation and robust support resources to help users get the most out of the solution.

6.1.7. Administration and Management Usability

The Solution shall have an easy-to-use administration console and allow straightforward ongoing management that utilizes a lightweight agent with low impact on potential performance.

RESPONSE:

Cisco Secure Endpoint delivers on these requirements by providing an easy-to-use administration console and a lightweight agent designed to minimize impact on performance.

Administration Console: The administration console for Cisco Secure Endpoint is designed to be user-friendly and intuitive. It provides a centralized location for managing all aspects of the solution, including policy setting, threat detection and response, and system configuration. The console offers a dashboard view that displays real-time information about the organization's security posture, allowing administrators to quickly understand and respond to security events. This console is also part of the SecureX platform, providing a unified experience across all Cisco security solutions.

Easy Management: Cisco Secure Endpoint simplifies the ongoing management of your endpoint security. Policy setting and updates are straightforward, with the ability to apply policies across multiple endpoints or tenants with a few clicks. Furthermore, any updates to the system or the endpoint agent software are automatically handled by the solution, reducing the administrative overhead.

Lightweight Agent: The endpoint agent for Cisco Secure Endpoint is designed to be lightweight and efficient, ensuring minimal impact on system performance. The agent operates quietly in the background, monitoring for threats and enforcing policies without interrupting the user's workflow. Despite its lightweight nature, the agent delivers robust security capabilities, including real-time threat detection and response, file trajectory tracking, and more.

Low Impact on Performance: The agent's design ensures that even during active scanning or incident response actions, the impact on system performance is kept to a minimum. This ensures that user productivity is not adversely affected, even while comprehensive security measures are in place.

In summary, Cisco Secure Endpoint provides an easy-to-use administration console and straightforward management capabilities, while the lightweight agent ensures robust security with minimal impact on system performance.

6.1.8. Endpoint Detection and Response

The Solution shall record system behaviors to detect suspicious events, investigate and block malicious activity, and contain malicious activity at the endpoint. The Solution shall use the data to investigate and provide remediation guidance for any affected systems.

RESPONSE:

Cisco Secure Endpoint uses advanced detection and response capabilities to record system behaviors, detect suspicious events, and effectively respond to and contain malicious activity.

Behavioral Analysis: Cisco Secure Endpoint monitors and records system behaviors across all endpoints. It uses machine learning and behavior-based analytics to detect any anomalies or suspicious events, even those caused by previously unseen threats. This continuous monitoring and recording provide a comprehensive view of activities at the endpoint level, allowing for effective threat detection and response.

Investigation and Blocking of Malicious Activity: When a suspicious event or behavior is detected, the solution can automatically investigate the source and nature of the threat. It can then take appropriate actions to block the malicious activity, which could include isolating the affected endpoint, terminating malicious processes, or removing malicious files.

Containment at the Endpoint: Cisco Secure Endpoint is designed to contain threats directly at the endpoint. By integrating prevention, detection, and response capabilities in a single agent, it can rapidly stop threats in their tracks, reducing the risk of lateral movement or data exfiltration.

Remediation Guidance: Following the detection and containment of a threat, Cisco Secure Endpoint (Premier) provides remediation guidance to help recover any affected systems. This guidance is informed by Cisco's extensive threat intelligence and can include specific steps to remove the threat, patch vulnerabilities, and prevent future infections.

Threat Hunting: Additionally, the solution also provides proactive threat hunting capabilities. Security teams can use the recorded data to search for indicators of compromise (IOCs), enabling them to identify and respond to potential threats before they can cause significant harm.

Integration with SecureX: When integrated with SecureX, Cisco's security platform, these capabilities are further enhanced. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions, allowing for coordinated threat response across your entire security infrastructure.

In summary, Cisco Secure Endpoint records system behaviors to detect and respond to threats effectively, containing malicious activity at the endpoint, and provides remediation guidance for affected systems.

6.1.9. Endpoint Protection Platform Suite

The Solution shall use an extended portfolio of security tools, like endpoint firewalls, device and application control, application inventory, signature matching, vulnerability and patch management and others, plus network-level tools such as secure email and sandboxing.

RESPONSE:

Cisco Secure Endpoint is designed to integrate and work seamlessly with an extended portfolio of security tools, both from Cisco and third-party vendors, enabling a holistic and comprehensive approach to security.

Device Control: Cisco Secure Endpoint includes device control capabilities that allow administrators to set policies to control the use of USB and other devices. This helps prevent potential data loss or introduction of malware through these devices. While it doesn't include an endpoint firewall, it can integrate with other network security solutions, including firewalls, to provide a multi-layered security approach.

Application Control and Inventory: The solution offers application control, allowing administrators to set policies on what applications can run on the endpoints. It also keeps an inventory of all applications running on the endpoints, helping organizations manage software licenses and identify potentially unwanted applications.

Signature Matching: Cisco Secure Endpoint uses signature matching as part of its multi-layered approach to threat detection. It checks files against an extensive database of known threat signatures to identify and block known malicious files.

Vulnerability and Patch Management: While Cisco Secure Endpoint does not include a built-in vulnerability and patch management system, it can integrate with other tools that provide these functions. It will provide visibility into vulnerabilities as part of its threat detection process, helping organizations prioritize their patching efforts.

Secure Email and Sandboxing: Integration with Cisco Secure Email can enhance protection against phishing and other email-based threats. Additionally, Cisco Secure Endpoint can utilize sandboxing technology to safely analyze suspicious files in an isolated environment.

Network-Level Tools: Integration with other network-level tools like Cisco Secure Network Analytics (formerly Stealthwatch) can provide additional visibility and threat detection capabilities.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Integration with SecureX: All these capabilities and integrations can be managed through SecureX, Cisco's security platform. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions, allowing for coordinated threat response across your entire security infrastructure.

In summary, Cisco Secure Endpoint leverages a broad portfolio of security tools to provide a comprehensive, integrated security solution. It works seamlessly with endpoint, network, and cloud security tools, providing a unified approach to threat detection, prevention, and response.

6.1.10. Operating System Support

The Solution shall protect a wide range of operating systems, including Windows, MacOS and Linux, and mobile operating systems like iOS and Android. The Solution shall provide specific functions for cloud, virtual and container-based workloads.

RESPONSE:

Cisco Secure Endpoint is designed to protect a wide range of operating systems and diverse environments, including cloud, virtual, and container-based workloads.

Operating System Support: Cisco Secure Endpoint supports a wide variety of operating systems. This includes Windows, MacOS, and various distributions of Linux for desktops and servers. It also extends support to mobile operating systems such as iOS and Android, ensuring comprehensive protection across all your devices.

Virtual Environments: Cisco Secure Endpoint is designed to work seamlessly in virtual environments. It ensures that your virtual machines are protected with the same level of security as your physical devices.

Integration with SecureX: These capabilities are enhanced when integrated with SecureX, Cisco's security platform. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions, allowing for a unified approach to security across your entire organization.

In summary, Cisco Secure Endpoint provides comprehensive protection across a wide range of operating systems and supports specific functions for cloud, virtual, and container-based workloads, delivering robust security no matter where your workloads reside.

6.1.11. Data Management and Storage

The Solution shall provide required data storage capacity, file types, and locations, as well as processes such as disaster recovery, rollbacks, extraction, or eradication.

RESPONSE:

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Cisco Secure Endpoint provides robust data handling capabilities to meet a variety of security requirements. It ensures data is stored securely and can be managed effectively, and provides features to support disaster recovery, rollbacks, extraction, and eradication.

Data Storage Capacity: Cisco Secure Endpoint, being a cloud-based solution, offers a significant amount of storage capacity for event data, logs, and other relevant security information. This data is stored in secure, geographically distributed data centers to ensure availability and resilience.

File Types and Locations: Cisco Secure Endpoint monitors and collects data on various file types and their locations on the endpoint. This information is crucial in investigating incidents, tracking file trajectories, and understanding the behavior of potential threats.

Extraction or Eradication: In the case of a detected threat, Cisco Secure Endpoint can isolate and eradicate the malicious files or processes on the affected endpoint. Additionally, suspicious files can be extracted for further analysis, either manually by security analysts or automatically via integration with other tools like a secure sandbox.

Integration with SecureX: When integrated with SecureX, Cisco's security platform, these capabilities are further enhanced. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions, allowing for a unified approach to security across your entire organization.

In summary, Cisco Secure Endpoint provides robust data storage and handling capabilities, supports a variety of file types and locations, and provides features such as disaster recovery, rollbacks, extraction, and eradication to effectively manage security incidents.

6.1.12. Performance Management

6.1.12.1. The Solution shall provide proactive alerts on system events, as well as logging and resolution reporting on all issues.

RESPONSE:

Cisco Secure Endpoint is designed to provide proactive alerts on system events and comprehensive logging and resolution reporting on all issues.

Proactive Alerts: The solution constantly monitors system events and provides real-time alerts when suspicious or malicious activities are detected. These alerts are designed to be actionable, providing administrators with the information they need to quickly understand and respond to the situation. Alerts can be customized based on severity, category, or other criteria to ensure that the security team focuses on the most critical issues.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Logging: Cisco Secure Endpoint logs all system events, including detections, actions taken, changes in system status, and more. This comprehensive logging helps provide visibility into system activities and is invaluable for incident investigation and response. The logs can be exported or integrated with other systems like SIEMs for further analysis.

Resolution Reporting: After an incident has been resolved, the solution provides detailed resolution reporting. This includes information on the nature of the threat, the endpoints affected, the actions taken to contain and eliminate the threat, and the final outcome. This information is crucial for understanding the effectiveness of the organization's security measures, compliance reporting, and improving future incident response efforts.

Integration with SecureX: Cisco Secure Endpoint can integrate with SecureX, Cisco's security platform. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions, allowing for a unified approach to security across your entire organization. This includes unified alerting and reporting, further enhancing the visibility and control over your security environment.

In summary, Cisco Secure Endpoint provides proactive alerts on system events, comprehensive logging, and detailed resolution reporting, helping your organization stay ahead of threats and effectively manage its security posture.

6.1.12.2. The Solution shall provide the ability to identify unhealthy agents on endpoints and self-heal issues. Any endpoints that cannot be self-healed must be reported through the administration console and reports.

RESPONSE:

Cisco Secure Endpoint is designed with capabilities to identify unhealthy agents on endpoints and undertake self-healing actions wherever possible.

Unhealthy Agent Identification: The solution constantly monitors the health status of the endpoint agents. If an agent is not communicating properly, not up-to-date, or experiencing other issues, it is identified within the console. This monitoring ensures that all agents are functioning optimally and providing the required security protection.

Self-healing Capabilities: When an unhealthy agent is detected, Cisco Secure Endpoint will first attempt to self-heal the issue. This could involve actions such as triggering an update or reapplying the security policy. These automated actions help to minimize the administrative overhead and reduce the window of exposure caused by unhealthy agents.

Reporting and Administration Console Alerts: If an agent cannot be self-healed, the issue is reported through the administration console. Alerts are generated to notify the administrators of the issue, ensuring that they can take immediate action. In addition, reports can be generated to

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

provide an overview of the health status of all agents in the network, helping to identify patterns or persistent issues that may need to be addressed.

Integration with SecureX: When integrated with SecureX, Cisco's security platform, these capabilities are further enhanced. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions, which includes a unified view of the health status of all agents and streamlined alerting and reporting functions.

In summary, Cisco Secure Endpoint provides the ability to identify unhealthy agents on endpoints, perform self-healing actions to resolve issues, and report any unresolved issues through the administration console and reports. This ensures that all endpoints are protected, and any issues are quickly identified and addressed.

6.1.13. Security

The Solution shall offer configurable controls that extend data and transaction security and compliance to third-party platforms or hosting providers the Solution uses. The Solution shall document security policies, audits, attestations, or evaluations for compliance needs.

RESPONSE:

Cisco Secure Endpoint is designed with robust controls and features that extend data and transaction security and compliance, even when interacting with third-party platforms or hosting providers.

Configurable Controls: The solution provides configurable controls that can be adjusted to meet your organization's specific security and compliance requirements. These controls can be applied to the data and transactions that interact with third-party platforms or hosting providers, ensuring that your security posture is maintained across all aspects of the solution.

Third-Party Integrations: Cisco Secure Endpoint can integrate with a variety of third-party platforms, and when it does, it maintains its commitment to security and compliance. Any data transmitted to these platforms is encrypted, and Cisco works closely with these partners to ensure they adhere to the same strict security and compliance standards.

Security Policies Documentation: Cisco Secure Endpoint includes a comprehensive set of documented security policies that detail the technical and procedural controls in place to protect your data. These policies cover a wide range of areas, including access control, encryption, incident response, and more.

Audits, Attestations, and Evaluations: Cisco maintains a robust compliance program that includes regular audits, attestations, and evaluations. These are conducted by independent third parties and cover various compliance standards. Reports from these audits are available to customers to support their own compliance efforts.

For more information, please visit: <https://trustportal.cisco.com/>

Integration with SecureX: When integrated with SecureX, Cisco's security platform, these capabilities are further enhanced. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions and includes features to help you manage and demonstrate your compliance.

In summary, Cisco Secure Endpoint offers configurable controls for data and transaction security and compliance, even with third-party platforms or hosting providers. It provides comprehensive documentation of its security policies, and supports compliance needs with audits, attestations, and evaluations.

6.1.14. Data Management

The Solution shall enable monitoring, reporting, and management of data sharing, as well encryption and security for data at rest and in motion.

RESPONSE:

Cisco Secure Endpoint provides robust capabilities for monitoring, reporting, and managing data sharing, as well as ensuring the security of data at rest and in motion.

Data Sharing Monitoring, Reporting, and Management: Cisco Secure Endpoint monitors data sharing activities on the endpoint devices. This includes tracking file accesses, transfers, and other activities that could indicate data exfiltration attempts. The solution provides reports on these activities, helping administrators identify potential data leaks and take appropriate action. Administrators can also set policies to control data sharing activities based on their organization's security requirements.

Data Encryption: Cisco Secure Endpoint ensures the security of data at rest and in motion through encryption.

Data at Rest: All data stored by the solution, whether it's in the endpoint devices or in the cloud, is encrypted using strong encryption algorithms. This includes event data, logs, configuration data, and any other data collected or used by the solution. The encryption keys are securely managed to prevent unauthorized access.

Data in Motion: All data transmitted by the solution, whether it's between the endpoint and the management server, or between the solution and third-party integrations, is encrypted. This ensures that even if the data is intercepted during transmission, it cannot be read by unauthorized parties.

Security of Data: In addition to encryption, Cisco Secure Endpoint uses other security measures to protect data. This includes access controls to ensure that only authorized users can access the data, and integrity checks to ensure that the data has not been tampered with.

Integration with SecureX: These capabilities are enhanced when Cisco Secure Endpoint is integrated with SecureX, Cisco's security platform. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions, allowing for a unified approach to security across your entire organization.

In summary, Cisco Secure Endpoint enables effective monitoring, reporting, and management of data sharing, and ensures the security of data at rest and in motion through encryption and other security measures.

6.1.15. Disaster Recovery and Backup

The Solution shall enable processes such as disaster recovery, rollbacks, and version control.

RESPONSE:

Cisco Secure Endpoint is designed with robust capabilities that support disaster recovery, rollbacks, and version control, ensuring the integrity and availability of your security infrastructure.

Disaster Recovery: As a cloud-based solution, Cisco Secure Endpoint ensures that your data is stored securely in geographically distributed data centers. In the event of a disaster, your data can be quickly restored from these data centers, minimizing downtime and data loss. Additionally, Cisco Secure Endpoint's cloud architecture ensures that the service remains available even if a particular data center experiences an outage.

Rollbacks: If an endpoint is compromised, administrators can use the system's historical data via endpoint forensic snapshots, to assist with reverting the endpoint to its pre-attack state. This forensic snapshot capability is crucial for recovering from a security incident and minimizing its impact.

Version Control: Cisco Secure Endpoint provides version control capabilities for its endpoint agents. Administrators can choose which version of the agent to deploy on the endpoints, allowing them to test new versions in a controlled environment before rolling them out across the organization. Furthermore, the solution keeps track of the version history, making it easy to identify and resolve issues related to specific versions.

Integration with SecureX: When integrated with SecureX, Cisco's security platform, these capabilities are further enhanced. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions, which includes unified management of disaster recovery, rollbacks, and version control.

In summary, Cisco Secure Endpoint enables processes such as disaster recovery, rollbacks, and version control, helping to maintain the integrity and availability of your security infrastructure.

6.1.16. Identity and Access Management

The Solution shall provide capabilities such as user authentication, password policy management, two factor authentication, single sign on, and role-based access.

RESPONSE:

Cisco Secure Endpoint is designed with robust capabilities for user authentication, password policy management, two-factor authentication, single sign-on, and role-based access control.

User Authentication: Cisco Secure Endpoint requires users to authenticate before they can access the system. This ensures that only authorized users can access the solution and its data.

Two-Factor Authentication (2FA): Cisco Secure Endpoint supports two-factor authentication, adding an additional layer of security to the authentication process. With 2FA, users are required to provide a second factor, such as a token or a biometric identifier, in addition to their password. This helps to prevent unauthorized access even if a user's password is compromised.

Single Sign-On (SSO): The solution supports single sign-on, allowing users to authenticate once and gain access to multiple systems. This not only improves user convenience but also helps to reduce the risk of password-related security issues.

Role-Based Access Control (RBAC): Cisco Secure Endpoint uses role-based access control to ensure that users only have access to the features and data they need to perform their roles.

Integration with SecureX: When integrated with SecureX, Cisco's security platform, these capabilities are further enhanced. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions, including unified management of user authentication, password policy, 2FA, SSO, and RBAC.

In summary, Cisco Secure Endpoint provides robust capabilities for user authentication, password policy management, two-factor authentication, single sign-on, and role-based access control, helping to ensure the security and integrity of your system.

6.1.17. Network

The Solution shall leverage network technologies like software-defined wide area networks and over-the-top monitoring to ensure the optimal performance of the Solution.

RESPONSE:

Cisco Secure Endpoint is a high-performance lightweight agent designed for minimal impact on the end-user device and on the network.

Integration with SecureX: When integrated with SecureX, Cisco's security platform, these capabilities are further enhanced. SecureX provides a centralized interface for managing and

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

monitoring all of Cisco's security solutions, including the ability to view and manage network performance data.

In summary, Cisco Secure Endpoint leverages network technologies like SD-WAN and OTT monitoring to ensure the optimal performance of the solution. This ensures that your security infrastructure is not only effective, but also efficient and user-friendly.

6.1.18. Compliance and Third-Party Certification

The Solution shall comply with relevant standards like General Data Protection Regulation (GDPR), Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act, Personally Identifiable Information (PII) data requirements, Driver Privacy Protection Act, and third-party certifications such as Systems and Organizations Controls 2 (SOC 2) and International Organization for Standardization (ISO) 27001. The Department, Purchaser, or Customer may require Contractor(s) to execute security agreements, including but not limited to, CJIS riders or Business Associate Agreements as a condition of performance or purchase order issuance.

RESPONSE:

Cisco Secure Endpoint is designed to comply with a wide range of data protection and privacy standards. Cisco maintains a robust compliance program that includes regular audits, attestations, and evaluations. These are conducted by independent third parties and cover various compliance standards. Reports from these audits are available to customers to support their own compliance efforts.

For more information, please visit: <https://trustportal.cisco.com/>

6.1.19. Configuration and Customization

The Solution shall allow customization of the standard deployed solution with custom user interfaces, data tables, process components, and business logic.

RESPONSE:

Cisco Secure Endpoint offers several ways to customize the standard deployed solution to better suit your organization's unique needs and preferences:

Custom User Interfaces: While the primary user interface for Cisco Secure Endpoint is designed to be intuitive and user-friendly, it also allows for some degree of customization. Administrators can customize dashboards, create custom views, and adjust settings to align with specific operational requirements.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Data Tables: Cisco Secure Endpoint allows administrators to customize the presentation of data within the console. They can apply filters, and sort data based on various criteria. This enables each user to focus on the information that's most relevant to their role.

Process Components: Workflow processes within Cisco Secure Endpoint can be customized to better align with your organization's incident response procedures. For instance, you can define custom actions to be taken when a certain type of threat is detected, tailoring the solution's response to your specific policies and procedures.

Business Logic: With Cisco Secure Endpoint's robust API (Application Programming Interface), you can extend the solution's capabilities and integrate it with other systems. This allows you to implement custom business logic, automate tasks, and create a security ecosystem that's closely aligned with your business operations.

However, it's important to note that these customization capabilities are balanced with the need to maintain the solution's integrity and security. While Cisco Secure Endpoint offers flexibility, certain core aspects of the solution cannot be modified to ensure it remains secure and effective.

As always, Cisco offers comprehensive support to assist with the customization and deployment of the solution, ensuring it aligns with your organization's specific needs and requirements.

6.1.20. Role-Based Access

Solution shall provide the ability to create customizable role-based personas based on responsibility.

RESPONSE:

Cisco Secure Endpoint supports the creation of customizable, role-based personas, enabling the system to align with the structure and responsibilities of your organization.

Role-Based Access Control (RBAC): Cisco Secure Endpoint uses role-based access control (RBAC) to manage user access to the system. Administrators can define role-based permissions to users. Each user has specific permissions that determine what actions they can perform and what data they can access in the system.

Easy Management: It is easy to assign and change user permissions. If a user's responsibilities change, their permissions can be quickly updated to reflect these changes.

Integration with SecureX: When integrated with SecureX, Cisco's security platform, these capabilities are further enhanced. SecureX provides a centralized interface for managing and monitoring all of Cisco's security solutions, which includes unified management of RBAC.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

In summary, Cisco Secure Endpoint provides the ability to create customizable role-based personas based on responsibility. This ensures that each user has the access they need to perform their job effectively, while minimizing the risk of unauthorized access.

6.1.21. Data Export

The Solution shall provide the ability to generate a customizable export of data based on platform user filters for assets, services, and issues present within the platform.

RESPONSE:

Cisco Secure Endpoint meets and exceeds the outlined requirements. Our solution provides a comprehensive, customizable data export feature that allows you to tailor data visibility based on your specific needs. Here's how it responds to each of your requirements:

Customizable export of data: Cisco Secure Endpoint provides a robust API that allows for the extraction of data from the system. This data can be customized based on the specific needs of the user, allowing for a high degree of flexibility in what data is exported.

User Filters for Assets: The solution provides comprehensive asset visibility across your entire organization. This includes the ability to view and filter assets based on a variety of criteria, including but not limited to asset operating system, IP addresses, hostnames, connector version, policy, groups, and more. This information can be readily exported based on the filters applied, enabling you to focus on the specific assets you are interested in.

User Filters for Issues: Our solution offers the ability to view and filter security events, issues, and incidents. This includes the ability to track these based on a variety of criteria including severity, status, and type. This data can also be exported based on the applied filters, providing you with the ability to focus on specific issues that are of interest to you.

In conclusion, Cisco Secure Endpoint provides a high degree of customization for data export, allowing you to focus on the specific assets, services, and issues that are relevant to you. This ensures that you have the data you need to make informed decisions about your security posture.

6.1.22. Integration

6.1.22.1.

The Solution shall integrate with the Department's existing security tools such as firewalls, antivirus software, endpoint management solutions and security information and event management (SIEM) systems. The Customer shall determine if the Solution is able to integrate with the Customer's security tools. The Contractor shall take any steps necessary to support Customer integration.

RESPONSE:

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Cisco Secure Endpoint is designed with interoperability in mind, allowing it to seamlessly integrate with a wide range of security tools. Here is how our solution matches your integration requirements:

Firewalls: Cisco Secure Endpoint integrates with popular firewall solutions, including Cisco's own firewall offerings, to facilitate information sharing and improve overall security posture. Alerts from the firewalls can trigger automatic responses in Cisco Secure Endpoint, allowing rapid response to detected threats.

Antivirus Software: Cisco Secure Endpoint is itself a robust antivirus solution providing both signature-based and behavior-based detection capabilities. However, if you have other preferred antivirus solutions in place, Cisco Secure Endpoint can integrate with them to provide additional layers of security.

Endpoint Management Solutions: Our solution integrates with leading endpoint management solutions, which enables better visibility and control over endpoints. By sharing data with these solutions, Cisco Secure Endpoint ensures a unified and streamlined approach to managing and securing devices.

Security Information and Event Management (SIEM) Systems: Cisco Secure Endpoint integrates smoothly with leading SIEM systems like Splunk, IBM QRadar, and others. By feeding rich endpoint detection and response data to these systems, it enhances their ability to identify threats and provide comprehensive security intelligence.

To ensure successful integration, Cisco provides detailed documentation and direct support from our team of experts. Furthermore, we are ready to work closely with your IT staff, provide necessary training and resources, and undertake any steps necessary to ensure seamless integration with your existing security infrastructure.

Cisco's aim is to collaborate with your organization to ensure that our solution fits your needs and integrates effectively into your existing security ecosystem, thereby enhancing your overall security posture.

6.1.22.2.

The Solution shall be capable of data integration through common exchange techniques and frameworks such as RESTful Application Programming Interfaces (APIs).

RESPONSE:

Cisco Secure Endpoint is designed to enable seamless data integration through common exchange techniques and frameworks, including RESTful Application Programming Interfaces (APIs).

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Our solution provides a well-documented, RESTful API that allows you to programmatically extract, push, and manipulate data from the platform. This ensures that you can smoothly integrate Cisco Secure Endpoint with other systems, tools, and applications in your environment.

With the RESTful API, you can:

Pull data: You can extract data related to threat intelligence, asset details, issue alerts, incident reports, and more. This data can be consumed by other systems or applications for further analysis, visualization, or action.

Push data: You can also send data to Cisco Secure Endpoint. This could include new asset details, updated configurations, or other relevant information.

Manipulate data: You can use the API to update the status of incidents, reclassify threats, initiate actions like system scans, and much more.

Using standard HTTP methods (GET, POST, PUT, DELETE), the RESTful API allows for easy integration and interaction with a wide range of systems. This design also ensures that it will remain compatible with future systems that use these standards.

In summary, Cisco Secure Endpoint's RESTful API is a powerful tool for integrating our solution into your existing data infrastructure, promoting data exchange, and enabling automation.

6.1.22.3.

The Solution shall be capable of integrating with a variety of identity and access management (IAM) systems to meet Customer current and future needs.

RESPONSE:

Cisco Secure Endpoint is designed to integrate smoothly with various Identity and Access Management (IAM) systems.

Our solution aligns with the SAML 2.0 protocol, an open standard used by many IAM solutions, which allows it to facilitate single sign-on (SSO) capabilities and integrate with a host of IAM platforms. Here are some examples:

Cisco's Own IAM - Duo Security: Cisco Secure Endpoint integrates seamlessly with Duo, Cisco's own IAM solution, providing an extra layer of security for user authentication.

Microsoft Active Directory (AD): Integration with AD allows for streamlined user and group management, enabling your IT staff to implement and maintain access policies more efficiently.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Okta: As one of the leading IAM solutions in the market, Okta integration allows for a secure, efficient user authentication process, and is especially beneficial for organizations already using Okta as their IAM solution.

Other SAML 2.0 Compatible IAM Systems: If your organization uses other IAM solutions that are compatible with SAML 2.0, Cisco Secure Endpoint can integrate with them to provide a secure and efficient access management solution.

Furthermore, Cisco is committed to future-proofing its security solutions. We continually update our products to stay in line with evolving security standards and protocols, ensuring that Cisco Secure Endpoint will be able to meet your future IAM integration needs.

Please note that the actual integration process and capabilities might vary based on the specific IAM system. However, Cisco's support team will be available to assist your organization through the integration process, helping to ensure a smooth transition and effective utilization of Cisco Secure Endpoint within your existing security infrastructure.

6.1.22.4.

Initial Integration shall include connecting each Customer to the state Cybersecurity Operations Center (CSOC) and validating with FL[DS] that all Solution data is properly integrated, as requested by the Customer.

RESPONSE:

Cisco Secure Endpoint can indeed be integrated with your state Cybersecurity Operations Center (CSOC). This integration is designed to enable centralized monitoring, threat intelligence sharing, and coordinated incident response, thus enhancing the overall cybersecurity posture of your organization.

The steps to achieve this are generally as follows:

Configuration of API Connections: The initial step involves configuring API connections between Cisco Secure Endpoint and your CSOC's system. The secure API provided by Cisco Secure Endpoint enables a two-way communication, ensuring that relevant data can be transferred in real-time or per a scheduled routine.

Data Mapping and Integration: The next step involves mapping the data from Cisco Secure Endpoint to the corresponding fields or data types in the CSOC's system. This process ensures that all important data—such as threat alerts, asset information, and incident reports—are accurately reflected in the CSOC's monitoring interface.

Testing and Validation: Once the integration is configured, we'll conduct thorough testing to ensure data is accurately transmitted and reflected in the CSOC's systems. This will include

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

validating the integration with your department (FL[DS]) to ensure that all solution data is properly integrated as per your requirements.

Finalization and Documentation: Once testing and validation are completed, the integration process will be finalized. Detailed documentation will be provided to ensure that your team understands how the data is transferred, what data is available, and how to troubleshoot any potential issues.

Cisco's dedicated support team will be available to guide you through this process, providing technical assistance, advice, and best practices to ensure successful integration.

It's worth noting that the exact process might vary depending on the specific systems and protocols your CSOC uses, but rest assured that Cisco Secure Endpoint is designed to be flexible and interoperable, ensuring it can integrate smoothly with your CSOC's systems.

6.1.22.5.

Integration Maintenance may be required after initial integration to ensure that the Solution properly exchanges data between Customers and the CSOC. The Contractor shall address any concerns that FL[DS] has regarding integration issues.

RESPONSE:

Cisco understands that maintaining the integration between Cisco Secure Endpoint and your Cybersecurity Operations Center (CSOC) is critical to ensure smooth and secure operations. To this end, we offer a comprehensive support package to address any concerns or issues that may arise post-integration:

Proactive Monitoring and Maintenance: Cisco monitors the health of its systems and the integrations with customer systems. In case of any disruptions or issues, proactive steps will be taken to rectify the situation and ensure the smooth exchange of data.

Support Team Availability: Our support team is available 24/7 to address any concerns or issues you may have. This includes technical issues, integration-related questions, or any other concerns regarding the solution.

Issue Resolution: In the event of any integration issues, our team will work closely with FL[DS] to understand the problem, diagnose the cause, and quickly find a solution. Our aim is to minimize any potential downtime and ensure that the solution continues to function as expected.

Regular Updates and Patches: Cisco regularly releases updates and patches for its products, including Cisco Secure Endpoint. These updates not only add new features and improvements but also ensure that the solution stays compatible with the systems it's integrated with, such as your CSOC.

Documentation and Training: Cisco provides comprehensive documentation and training resources to help your team understand the integration better and troubleshoot minor issues themselves. This empowers your team to maintain the integration effectively.

Consultation for Changes: If there are changes in your environment, such as upgrades or changes to the CSOC systems, Cisco will provide consultation and assistance to ensure that the integration with Cisco Secure Endpoint continues to function smoothly.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

In summary, Cisco is committed to ensuring that the integration between Cisco Secure Endpoint and your CSOC stays functional and efficient, and we are ready to address any concerns that FL[DS] may have regarding integration issues.

a) DRAFT SLA

RFQ Text:

A draft SLA for Solution performance and availability which adheres to all provisions of this RFQ.

Response:

The Service Description for Cisco Secure Endpoint is inserted below.

b) TRAINING & SUPPORT SLA

RFQ Text:

A draft SLA for training and support which adheres to all provisions of this RFQ.

i. The training SLA must specify initial training (included in Item No. 1 on Attachment A, Price Sheet) provided and ongoing training provided (included in Item No. 2 on Attachment A, Price Sheet).

Response:

Cisco offers free on-demand online training. In addition, Cisco offers optional individual training class as described below:

Course: Protecting Against Malware Threats with Cisco AMP for Endpoints (SSFAMP) v6.0

The Protecting Against Malware Threats with Cisco AMP for Endpoints (SSFAMP) v6.0 course shows you how to deploy and use Cisco Advanced Malware Protection (AMP) for Endpoints, a next-generation endpoint security solution that prevents, detects, and responds to advanced threats.

Through instructor videos and hands-on lab exercises, you will learn how to implement and use this powerful solution through a number of step-by-step attack scenarios. You'll learn how to build and manage a Cisco AMP for Endpoints deployment, create policies for endpoint groups, and deploy connectors. You will also analyze malware detection using the tools available in the AMP for Endpoints console, Cisco Threat Grid, and the Cisco Orbital Advanced Search Tool.

Price: \$1000 per person

c) IMPLEMENTATION PLAN

RFQ Text:

Florida Digital Service
 RFQ Title: Endpoint Detection and Response Solution
 RFQ Number: DMS-22/23-155
 Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

A draft implementation plan for a Customer which adheres to all provisions of this RFQ.

Response:

Included in the Price Sheet is an initial implementation based on a fixed scope of endpoints, details below. Price per Entity: \$25,000

Cisco Secure Endpoint Initial Implementation

Scope includes:

- Configuration of Cloud portal
- Endpoint connectors
 - Install connector agent on endpoint, and validate
 - 3 connectors – for example, mobile device, windows, mac (workstations only)
 - ◇ Does not include servers
- Deployment of endpoint on five (5) representative devices, to be deployed in monitor mode then moved to blocking mode after 1 week of monitoring
 - Client will be responsible for the deployment of the remaining clients
- Configuration of three (3) Audit and Protect Policies
- Configuration of three (3) Device groups
- Perform one (1) connector package push for up to six (6) endpoints

1.1.1. Client responsibilities:

- Work with Presidio to define Secure Endpoint policies
- Identify and agree upon the (5) test deployment endpoints
- Facilitate troubleshooting, validation, and configuration adjustments to the deployed test endpoints
- Work with Presidio to identify and agree upon the limited production deployment endpoints
- Client is responsible for mass deployment via client provided GPO/MDM solution
- Client is responsible for configuration (including removal) of any existing endpoint security product integrations

Optional add on: Presidio has additional implementation services available to assist FLDS or Entities at an hourly rate at \$250/hour. We can offer guidance on quantities of hours needed, based on guidance from FLDS and potential level of effort for participating entities, on a Time & Materials (“T&M”) basis. Logistics and timing can be coordinated with participating parties and FLDS.

d) MDR SLA (OPTIONAL)

RFQ Text:

A draft MDR SLA, if applicable, per section 6.6.1 with annual pricing

Response:

MDR is available for 500 licenses or more of Cisco Secure Endpoints. Once that threshold is met the pricing is available in a waterfall format, listed below. The MDR SLA and details can be found after the pricing detailed below.

Cisco Secure Managed Detection and Response (MDR) Service for Endpoint

Florida Digital Service
 RFQ Title: Endpoint Detection and Response Solution
 RFQ Number: DMS-22/23-155
 Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Device Quantity	Rate Per Device	Annual MDR Rate (in addition to EDR purchase)
500	\$5.67	\$34,020.00
1000	\$3.88	\$46,560.00
5000	\$2.77	\$166,200.00
10000	\$2.34	\$280,800.00
25000	\$1.94	\$582,000.00

e) FUTURE INTEGRATIONS SLA (OPTIONAL)

RFQ Text:

A draft SLA for future integrations, if applicable, per section 6.6.2 with pricing.

Response:

Cisco Secure Endpoints has existing integrated dashboards into ServiceNow. In addition, Cisco Secure Endpoints has readily available integration into ReliaQuest GreyMatter.

Cisco's partner ecosystem helps users expedite their investigations by identifying which endpoints have seen a file, creating custom file lists, and moving endpoints in and out of triage groups. All events generated in an environment can be collected and archived, allowing for extended historical data correlation. There are many 3rd party integrations, with more detail listed here: <https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/AMP-endpoints-partners-integrations.html#%7Ebenefits>

f) DISASTER RECOVERY PLAN

RFQ Text:

A draft disaster recovery plan per section 30.5.

Response:

Cisco Secure Endpoint aligns with the FLDS DR plan. Cisco's solution is hosted in 11 data centers, with 99.999% uptime. Below are details from Cisco's Business Continuity plan, also found here: <https://www.cisco.com/c/en/us/about/business-continuity.html>

Program Overview:

Q: Describe Cisco's overall business resiliency strategy

A: The business resiliency program is committed to providing a readiness state for the company that protects Cisco's top priorities:

- Employees
- Business operations

- Customers and partners
- Community
- Shareholders

The [Business Continuity Management policy](#) calls for reviews, updates, and testing of Business Continuity Plans at scheduled intervals. Cisco's Business Continuity Management strategy includes prioritizing key processes and functions utilizing Business Impact Analyses for processes and Service Impact Analyses for applications supporting business processes. Each of the critical processes and applications has resiliency plans to restore their functionality.

Q: What type of scenarios or business interruptions does Cisco plan for as part of its business resiliency program?

A: As part of our best practices approach, Cisco does not plan for specific scenarios. However, the company reviews and prioritizes the recovery of the critical processes, systems, and vendors that may be impacted during any disruptive event via an all hazards approach. With this approach, we capture the relevant elements to work effectively within any scenario.

Q: Does Cisco have a dedicated team of professionals focused on business continuity and disaster recovery?

A: Yes, Cisco has a dedicated Global Risk Management department within the finance organization. One of this department's responsibilities is governance of the cross-functional teams to ensure adherence to business continuity plans and testing. Another department, Safety, Security, and Business Resiliency, is responsible for Cisco's incident management program, and helps ensure the proper programs and operations are in place to support Cisco's Business Continuity Management strategy and execution. Both Global Risk Management and Safety, Security and Business Resiliency partner with various business functions to address the immediate crisis and ensure the continuation of Cisco's business.

Resiliency Planning:

Q: In the event of a disaster or significant disruption, does Cisco have documented business continuity plans?

A: Yes, Cisco maintains a set of business continuity plans to help us prepare and react appropriately if faced with external events outside of our control that could disrupt our business. In the event of a disruption, Cisco has a multitiered incident management program that is designed to assess and deal with potential disruptions globally. The program guides decision points for the activation and execution of recovery plans for processes and functions.

Q: In the event of a disaster or significant disruption to critical business processes, does Cisco have documented plans for recovering critical business processes and IT?

A: Yes, Cisco's business continuity plans are designed to recover critical business processes and functions identified in our Business Impact Analyses. In addition, Service Resiliency Plans (SRPs) for recovering IT services that support critical business

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

processes are based on a prioritization process based on their criticality as identified in the Business Impact Analyses. Cisco IT supporting services are categorized into five criticality bands to help ensure the most critical supporting services have documented plans in place to meet the associated service level agreements.

Q: Has Cisco incorporated any specific guidelines or provisions for pandemic influenza in their business continuity plans?

A: Cisco maintains a cross-functional Pandemic Influenza Global Planning Committee to address business, customer, and employee concerns. Led by Safety, Security and Business Resiliency and Global Risk Management, this team includes Cisco representatives from human resources including medical, communications, legal, workplace resources, environmental health and safety, global protective services, and information technology.

The Pandemic Influenza Global Planning Committee is responsible for maintaining the pandemic plan, which includes response plans, communication strategies, and educational awareness. Cisco regularly monitors pandemic-related information and alerts from the Centers for Disease Control (CDC) and the World Health Organization (WHO).

Q: Describe Cisco's process for reviewing and signing off on business continuity plans

A: Cisco's business continuity plans are reviewed and approved by the sponsors of each of the business functions for which plans have been implemented. The plans are also reviewed by Cisco's internal audit teams and as part of select external audits.

Q: How often does Cisco update or review its business continuity plans?

A: It is the responsibility of each business plan owner to complete an annual review and update appropriately. If a material change occurs in the business operations, the plans are to be updated sooner.

Q: Will Cisco provide customers with a copy of the current business continuity plans?

A: Because of the confidential nature of the material they contain, Cisco does not share its business continuity plans with individuals outside the organization. Under certain circumstances, and with non-disclosure agreements (NDAs) in place, Cisco is willing to provide summary information or meet with parties interested in discussing specific parts of the plans.

Q: In the event of a disaster, does Cisco have business continuity plans to address services and products provided to customers that can meet their business recovery requirements?

A: Cisco maintains a network of 24-hour Technical Assistance Centers (TACs) and service parts distribution centers to provide services and support to customers. These globally distributed centers are able to balance a peak workload if one or more sites are impaired. Regional business continuity plans are in place to support and recover global TAC operations.

Testing / Exercising

Q: What is Cisco's overall business resiliency testing strategy?

A: Business continuity plans are tested as part of a maintenance process by each of the business owners. Data restoration plans are also tested in conjunction with business

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

operations and are embedded as part of IT operations teams. When new business operations are established, table top tests are performed as part of the plan development and initial implementation stage.

Once tests are complete, there are corrective actions for any observed deficiencies. Business continuity plans are approved by management following each update. Each business continuity team is expected to conduct an annual exercise. Exceptions can be made only when a team has responded to an actual event during the course of the year which invoked its business continuity plan.

Q: Do internal or external auditors review Cisco's business continuity and disaster recovery tests?

A: Yes, internal and external auditors may review business continuity plan and SRP test results as a part of annual audit activities.

Q: How often does Cisco test its business continuity plans?

A: Business continuity plans are tested when the plans are first created, and as part of annual update and maintenance cycles.

Q: Will Cisco share its test results or conduct joint tests with customers?

A: Cisco's test results are proprietary and are not shared with external parties. We generally do not engage in joint testing, except as it relates to our suppliers, vendors, and critical partners.

Incident Management:

Q: Does Cisco have a documented company-level incident management plan that covers internal and external communications during a disruption?

A: Yes, Cisco has a global incident management plan in place, as well as incident management teams at the executive, global, regional, and local levels. These teams make and direct strategic decisions based on input from the functional team representatives. The incident management teams have functional representatives from more than 17 different groups within Cisco.

An activated incident management team serves as the focal point for information gathering and decision making for the execution of the incident management response. Internal and external communications are addressed as part of these plans and specific teams are dedicated to addressing communications needs. The functional incident management teams have responsibility for declaring a disaster within Cisco and invoking the business continuity plans as needed.

Q: How will customers be notified if a disaster at Cisco were assessed as affecting contracted services and products?

A: Your Cisco sales account team will be your primary point of contact and will be responsible for communications about any Cisco business impairment that could impact customers directly. Communications are initiated within the Incident Management Team and managed as part of the Incident Management Team communications plans.

Q: Will Cisco provide a copy of its incident management plan?

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

A: Because the material is confidential, Cisco does not share its response plan with individuals outside the organization. Under certain circumstances, with the appropriate nondisclosure agreements in place, Cisco is willing to provide summary information or meet with parties interested in discussing specific parts of the plan.

IT Resiliency Strategies

Q: Does Cisco have a system recovery plan for critical systems?

A: Cisco has developed disaster recovery plans for critical applications and services supporting business processes. Additionally, system redundancy is built into the infrastructure of the data systems.

Q: Does Cisco have an alternative site location for data center recovery purposes?

A: Cisco operates development and production data centers around the world. As part of the company's global data center strategy, the company has adopted a paired data center model with a specific architecture to allow maximized network and application resiliency. Prioritization based on the five criticality bands governs aggregated outage and data triage.

In the event of a major disaster, Cisco's key environments can failover to disaster recovery facilities located in Raleigh, North Carolina.

Q: What is Cisco's expected recovery time for your critical business functions?

A: Cisco's recovery time objectives (RTO) are set by identifying which of the five criticality bands the business process falls within via the Business Impact Analysis. These RTOs are based on mission critical operations that include customer support, production, and revenue generation.

Q: Is Cisco's main IT facility or data center located in the same building or office complex occupied by your main business or operations staff?

A: No, Cisco operates development and production data centers worldwide. Most production is run out of North America where there are two primary data centers in San Jose, California, one in Mountain View, California, and two in Richardson, Texas. Some production is also run out of a pair of data centers in Amsterdam. While some of these are co-located with other Cisco offices, others are standalone. IT operations and teams are global and can support local or remote production data centers.

Recovery Strategies:

Q: Does Cisco have a workplace recovery plan for its critical sites?

A: Cisco's main campus is spread out over 40 buildings in San Jose, California. In addition, key operations are distributed globally at campus locations. Due to this dispersion of locations, our plans provide flexibility in relocation strategies and are not tied to single sites. We do not employ commercial recovery sites.

Q: Do Cisco's recovery plans cover all sites that you provide contracted services and products from?

A: Yes, our recovery plans for critical processes or functions including customer support (TAC), service logistics, and distribution are on a 24-hour customer support model.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Each global site in which a critical function or process resides is included in the function's recovery plans.

Q: Describe the relevant geographical distances pertaining to Cisco's backup facilities

A: Cisco's primary data centers in San Jose, California, and Richardson, Texas are geographically distinct from our alternate data center in Raleigh, North Carolina. Additionally we have production data centers distributed globally supporting regions of our global operations. Data center locations in the United States are staffed by IT operations. Business operations are located in separate buildings across our sites.

2) EXPERIENCE

RFQ Text:

Documentation describing any experience providing the Solution, or similar Solution, on a statewide basis or across a large geographic region.

Response:

Cisco Secure Endpoints currently protects State Governments, Local/City Municipalities, Higher Education, Fortune 100 Companies, and mid-tier to small enterprises.

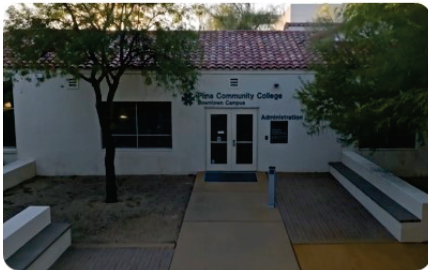
Industry Analyst and User Validation for Secure Endpoint

- Secure Endpoint was placed in the “Visionary” quadrant in the [2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms \(EPP\)](#) published in December 2022.
- Cisco was named a [Strategic Leader for Endpoint, Protection and Response in the AV Comparatives EPR Report](#) published on October 2022. As noted by AV-Comparatives; “AV-Comparatives’ Endpoint Prevention and Response Test is the most comprehensive test of EPR products ever performed.” In this report, AV-Comparatives evaluated the ability of 10 endpoint security products to detect or automatically block 50 unique targeted attacks, and Secure Endpoint:
 - Clearly achieved the highest ranking of 100 percent.
 - Was the only vendor with 100 percent in all phases, for both active and passive responses, for all 50 separate targeted attack scenarios.
 - Delivered the lowest TCO out of 10 products with a 5-year TCO of \$587 per agent.
- Cisco commissioned Forrester Consulting to perform an unbiased cost-benefit analysis of Secure Endpoint. The [Total Economic Impact \(TEI\) report](#) published in October 2022 found that:
 - Organizations using Secure Endpoint achieved an ROI of up to 287 percent and saw payback in less than six months.
 - After deploying Secure Endpoint and SecureX, organizations reduced the time to investigate and/or remediate by 50 percent.
 - Customers modernized their security and reduced their risk of material breach and productivity loss, with total benefits of \$2.25 million.

Cisco Secure Endpoint Case Studies and Testimonials

Case Studies

Pima Community College



Securing Campuses with Cisco Secure

Pima Community College trains the adult workforce across 11 campuses through in-class, remote, and hybrid classes. Before Cisco, Pima lacked a consistent network infrastructure and a coherent security architecture. Resource inventory was lacking, devices weren't accounted for, and many resources like classrooms were outside the security surveillance radar. Pima's security journey started with Cisco SecureX integrated with Cisco Secure Endpoint, Cisco Umbrella, and Cisco Secure Malware Analytics. And within months, Pima began to see the results.



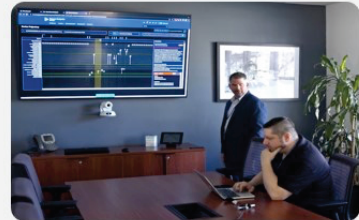
Challenges

- Lack of security baseline and visibility
- Lack of security telemetry due to inconsistent data
- Lack of security automation and orchestration capability
- Lack of a trusted partner to support Pima's small security team



Solutions

- Cisco Secure Endpoint
- Cisco SecureX
- Cisco Identity Services Engine (ISE)
- Cisco Umbrella
- Cisco Secure Malware Analytics
- Cisco Secure Access by Duo
- Cisco Secure Client



Outcomes

- Improved security posture for Pima's network infrastructure
- Reduced alerts from hundreds to a few
- Saved time on investigations and remediation
- Gained unified visibility regardless of user and device location
- Achieved advanced threat detection and response capabilities

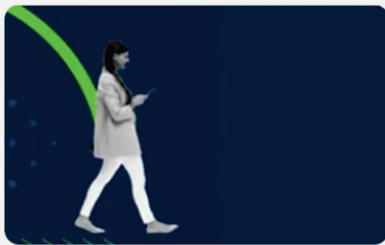
Read more [here](#).

Norwegian University of Science and Technology



Secure Endpoint Supports an Academic Community with Proactive Security

A renowned center for tech education, research, and innovation, NTNU serves 42,000 students and 9000 staff and faculty. Secure Endpoint's cloud-delivered endpoint protection, along with advanced endpoint detection and response, has enabled the security team to rapidly detect, contain, and remediate advanced threats. Orbital Advanced Search further simplifies security investigations and threat hunting.



Challenges

- Large footprint including 110,000 endpoints connecting to the network daily
- Unique environment with different stakeholders and needs
- Inconsistent visibility because staff and students are located around the world



Solutions

- Cisco Secure Endpoint
- Cisco SecureX
- Cisco Umbrella



Outcomes

- Gained unified visibility regardless of user and device location
- Improved advanced threat detection and response capabilities
- Reduced investigation and remediation time by 83%

Read more [here](#).

Testimonials



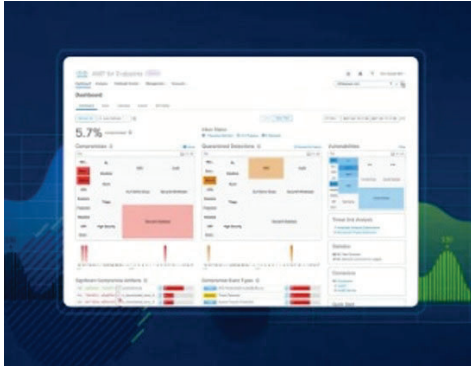
Cisco Provides Robust and Predictable Security

"Secure Endpoint's powerful EDR capabilities provided accurate telemetry for the devices and, in one case, detected the artifact of a ransomware infection simply based on the encrypted file for that ransomware."

Scott McGowan, Security Architect, Pima Community College

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®



Cisco Secure Helps You Do More with Less

"We needed an endpoint solution that could work with our user base distributed all over the world at any time and enable the SOC to handle incidents wherever the user might be [...] Secure Endpoint delivers better detection, faster analytics and correlations, and a faster response to threats that are not yet known to the global security community."

Christoffer Vargtass Hallstensen, Head of the Security Operations Center, NTNU

Read more [here](#).

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

3) IMPLEMENTATION

RFQ Text:

Documentation describing the vendor's capacity and ability to implement the Solution on a statewide basis.

Response:

Presidio and Cisco are prepared to support FLDS and other entities within Florida with a robust team of engineers, project managers, and architects. Presidio has 150+ field engineers spread across Florida, along with a NOC/SOC in Orlando Florida.

Presidio provided a standard implementation for a limited scope to stand up the Cisco Secure Endpoint solution including policies as identified in the Scope. Presidio has additional implementation services available to assist FLDS or Entities at an hourly rate at \$250/hour. We can offer guidance on quantities of hours needed, based on guidance from FLDS and potential level of effort for participating entities, on a Time & Materials ("T&M") basis. Logistics and timing can be coordinated with participating parties and FLDS.

4) VALUE-ADDED SERVICES

RFQ Text:

Detail regarding any value-added services.

Response:

Presidio Value-Added Services

Presidio is offering free Cybersecurity Framework Workshops to FLDS and all participating Entities. The workshops can be branded as “FLDS powered by Presidio” or performed on an individual basis upon direction by FLDS.

We find that organizations need a comprehensive approach to cybersecurity, but it is challenging to know where to begin. With multiple, overlapping tools deployed in the enterprise, it can be difficult to see the whole picture. Cybersecurity talent and leadership are tough to recruit and retain. Frequent turnover has caused many gaps in enterprise strategies and solutions. Presidio’s workshop will help Entities understand how to leverage the tools they are receiving from the FLDS Local Grant Program, how they fit into their existing environment, and provide guidance on a broader Cybersecurity strategy and/or roadmap.

The Cybersecurity Framework Workshop (“CSF360”) is based on the NIST-CSF Framework and designed to help document and provide a consultative, flexible and comprehensive approach to security operations enterprise-wide.

Cybersecurity experts from Presidio lead a high-level discussion to identify risks and opportunities to improve an organization’s cybersecurity posture. We will lead a discussion and interview your team in a group setting. Our experts will help you find the gaps in your security technology solutions and business processes. We will document our findings in a live whiteboard session and provide our expert recommendations to improve security operations enterprise-wide.

The Presidio CSF360 Cybersecurity Workshop explores all areas of an organization’s cybersecurity situation. It forms the foundation of a deeper discussion of potential risk elements.

- Uses the industry standard NIST Framework methodology to help gauge organization’s cybersecurity maturity
- Brings together stakeholders from multiple IT disciplines to discuss key cybersecurity initiatives
- Helps the organization gain a 360-degree view of their cybersecurity posture in just a few short hours
- Provides a high-level deliverable upon Workshop completion with recommended actions

The Presidio CSF360 Cybersecurity Workshop is generally completed in 2-4 hours with the participation of key stakeholders in the organization.

KEY BENEFITS

Florida Digital Service
 RFQ Title: Endpoint Detection and Response Solution
 RFQ Number: DMS-22/23-155
 Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Organizations who engage with Presidio’s CSF360 Workshop have dramatically enhanced their cybersecurity posture.

- Organizations that may have a security project roadmap but no formal way of measuring progress
- Organizations that have done self-assessments but would like another pair of eyes to review their efforts
- Organizations that have policies but may not be following them as closely as they would like
- Organizations that have regulatory concerns

They have created consensus across their organization about the people, processes and tools required to protect their business.

- Security Leadership: CISO, CSO, CIO, CXO
- Security Team: Architecture, Engineering, Operations,
- SOC, Analyst
- Networking Team, Firewall Admins
- Data Center Team, Directory Server Admins, Email, Identity, Access
- Application Team, DevOps, SRE

With a short investment in time and exploring the current situation, organizations will benefit from having a common ground for cybersecurity risk management.

- A list of Cybersecurity activities that can be customized to meet the needs of any organization
- A complementary guideline for an organization’s existing cybersecurity program and risk management strategy
- A risk-based approach to identifying cybersecurity vulnerabilities
- A systematic way to prioritize and communicate cost- effective improvement activities among stakeholders
- A frame of reference on how an organization views managing cybersecurity risk management

WHAT MAKES US DIFFERENT

Presidio is a trusted partner to our clients, securing their infrastructure, employees, clients, and assets from ever-growing cyber threats. Our clients trust Presidio:

- Highly Experienced team – Presidio's highly- credentialed cybersecurity consultants collectively have decades of combined practical experience spanning cyber security governance, architecture, and operations

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

- Proven Cyber Leadership – Presidio has 15+ years of providing cybersecurity leadership and securing our nations’ most sensitive networks with specialization across many of the largest industry verticals
- Business Enablers – We understand cybersecurity should reduce risk to enable the success of your business, not serve as a roadblock to your success

WHY PRESIDIO

Presidio is a leading digital systems integrator, with deep experience in networking, cloud computing and broad hybrid infrastructures. Presidio recognizes that cybersecurity is foundational to the success of any business and has a highly specialized expert team at the ready. Our clients benefit from:

- Services methodology built on recognized industry standards including NIST, CIS, and ISO
- Compliance depth & breadth including PCI, HIPAA, NERC CIP, GDPR, CCPA, SOC 2, ISO 27001, DFARS 800-171, CMMC
- Multi-discipline experts provide for a broad view of client’s potential vulnerabilities
- Deep cybersecurity services bench and broad security services solutions provide domain expertise and consistent deliverables

Presidio Cybersecurity Practice covers a broad security services portfolio. Our highly skilled and tenured cybersecurity practitioners maintain leading industry certifications, provide thought leadership and practical industry experience. We have conducted thousands of engagements across all major industry segments. We look forward to the opportunity to serve Florida Digital Service.

Florida Digital Service
 RFQ Title: Endpoint Detection and Response Solution
 RFQ Number: DMS-22/23-155
 Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

5) ATTACHMENT A – PRICE SHEET

RFQ Text:

Price Sheet, containing pricing for all items and completed in accordance with the instructions provided in this RFQ.

Response:

ATTACHMENT A PRICE SHEET

I. Alternate Contract Source (ACS)

Check the ACS contract the Quote is being submitted in accordance with:

_____ 43210000-US-16-ACS Technology Products, Services, Solutions, and Related Products and Services

_____ 43230000-NASPO-16-ACS Cloud Solutions

_____ 43230000-23-NASPO-ACS Software Value Added Reseller (SVAR)

II. Pricing Instructions

The vendor shall provide fixed rates quoted at or below the rates in the applicable ACS contract selected in Section I above. FL[DS] anticipates purchasing the external-facing asset discovery Solution for FL[DS] and all Customers. The estimated quantities listed are given only as a guideline for preparing the Quote and should not be construed as representing actual quantities to be purchased. No matter the quantity, the vendor may not exceed the quoted unit price. The Department reserves the right to utilize the quoted unit pricing during the term of the ATC and PO. Prices are ceiling rates inclusive of any and all costs associated with providing services.

III. Pricing

Initial Term Pricing (Years 1-3)		
Item No.	Description	Rate Per Device
1	<p>Initial Software Year</p> <p>One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance 	<p><u>\$ 38.84 per device*</u></p> <p><u>\$25,000 implementation per Entity</u></p> <p><u>*waterfall price available for higher quantities</u></p>

Florida Digital Service
 RFQ Title: Endpoint Detection and Response Solution
 RFQ Number: DMS-22/23-155
 Date Due: May 19, 2023, 5:00 PM EST



	<ul style="list-style-type: none"> • support services 	
2	<p>Subsequent Software Year</p> <p>One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance 	\$ 42.72 per device
Optional Renewal Term Pricing (Years 4-6)		
Item No.	Description	Rate Per Device
1	<p>Initial Software Year</p> <p>One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	<p>\$ 47.00 per device*</p> <p><u>\$25,000 implementation per Entity</u></p> <p><u>*waterfall price available for higher quantities</u></p>
2	<p>Subsequent Software Year</p> <p>One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ 51.70 per device

License Transferability: Should licensing transfer be required, Cisco will support the licensing transfer during the renewal cycle with the Entity/Purchaser. All existing domain data, log data, and content, will be preserved and transferred to the Entity/Purchaser.

Cisco supports the requirement in Section 33.0, Location of Data, of the RFQ to comply with Rule 60GG-4.002, F.A.C.; confirming data will not leave the United States per Rule 60GG-4.002, F.A.C.

Florida Digital Service
 RFQ Title: Endpoint Detection and Response Solution
 RFQ Number: DMS-22/23-155
 Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Software will be available to Customer within 3 business days after a PO is received from Purchaser.

Renewals are shown at a ceiling rate of 15% increase year over year. Actual renewal rate may be lower than ceiling rate.

IV. ACS Price Breakdown

In the table below, the vendor shall provide the pricing breakdown to document the pricing is in accordance with the applicable ACS contract. The vendor shall provide the ACS SKU Numbers, ACS SKU Descriptions, Market Price, and ACS Price that encompass the services as described in the RFQ:

Item No. 1 - ACS Pricing Breakdown for 43220000-NASPO-19-ACS (including implementation)				
ACS SKU Number	ACS SKU Description	Market Price	ACS Price	FLDS Price
AMP4E-SEC-SUB	Cisco Secure Endpoint XaaS Subscription	\$0	\$0	\$0
SVS-AMPE-SUP-E	Cisco AMP for Endpoints Enhanced SW Service	\$1	\$0.90	\$0.48
AMP4E-PRE-CL-LIC	Cisco Secure Endpoint Premier Tier Subscription	\$93.21	\$83.89	\$38.36
TG-AMPADV-K9	Cisco Secure Malware Analytics Cloud for Endpoint Advantage	\$0	\$0	\$0
CX-SEC-MDR	Cisco Secure Managed Detection and Response Service	\$0	\$0	\$0
SVS-MDR-EP	Cisco Secure MDR for Endpoint	\$7.45	\$6.70	\$5.67
PS-SVC-TM	Hourly for Presidio employee labor	\$743.17	\$661.17	\$225.00

Item No. 2 – ACS Pricing Breakdown for 43220000-NASPO-19-ACS (without implementation)				
ACS SKU Number	ACS SKU Description	Market Price	ACS Price	FLDS Price
AMP4E-SEC-SUB	Cisco Secure Endpoint XaaS Subscription	\$0	\$0	\$0
SVS-AMPE-SUP-E	Cisco AMP for Endpoints Enhanced SW Service	\$1	\$0.90	\$0.48
AMP4E-PRE-CL-LIC	Cisco Secure Endpoint Premier Tier Subscription	\$93.21	\$83.89	\$38.36
TG-AMPADV-K9	Cisco Secure Malware Analytics Cloud for Endpoint Advantage	\$0	\$0	\$0
CX-SEC-MDR	Cisco Secure Managed Detection and Response Service	\$0	\$0	\$0
SVS-MDR-EP	Cisco Secure MDR for Endpoint	\$7.45	\$6.70	\$5.67

V. Waterfall Pricing (Optional)

The Department is seeking an optional waterfall pricing model which leverages volume discounts. Vendors are encouraged to provide a pricing structure which specifies a volume range at which larger discounts could be applied. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

Device Quantity	Rate Per Device	Implementation Services per Entity	Annual Combined Rate (Device Rate + Support + Implementation*)
100	\$39.15	\$25,000	\$28,914.60

Florida Digital Service
 RFQ Title: Endpoint Detection and Response Solution
 RFQ Number: DMS-22/23-155
 Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

500	\$32.76	\$25,000	\$41,387.68
1000	\$31.36	\$25,000	\$56,361.40
5000	\$29.15	\$25,000	\$170,759.56
10000	\$23.14	\$25,000	\$256,489.84
25000	\$20.64	\$25,000	\$541,052.84

Optional MDR Price – add on to EDR rates above:**

MDR is available for 500 licenses or more of Cisco Secure Endpoints. Once that threshold is met the pricing is available in a waterfall format, listed below.

Cisco Secure Managed Detection and Response (MDR) Service for Endpoint		
Device Quantity	Monthly Rate Per Device	Annual MDR Rate (in addition to EDR purchase)
500	\$5.67	\$34,020.00
1000	\$3.88	\$46,560.00
5000	\$2.77	\$166,200.00
10000	\$2.34	\$280,800.00
25000	\$1.94	\$582,000.00

**** MDR ACS SKUs are listed in IV ACS Price Breakdown: CX-SEC-MDR and SVS-MDR-EP**

VI. State of Florida Enterprise Pricing (Optional)

The Department is also seeking an optional annual fixed rate to provide the Solution and services to all potential FL[DS] Customers. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

Cisco is willing to provide Enterprise Pricing upon more details for quantities and participating entities.

VII. Value-Added Services (Optional)

If vendors are able to offer additional services and/or commodities for external-facing asset discovery, at no additional cost to the Department, the vendor may offer the Department value-added services, in addition to the services and/or commodities expressly sought by this RFQ.

Presidio is offering a free 2 – 4 hour Cybersecurity Workshop to FLDS and each participating Entity upon request.

Per **Section 31.0**, Scrutinized Companies, a vendor submitting a Quote must certify that their company is not participating in a boycott of Israel. By signing below, the vendor so certifies. Additionally, the person submitting the quote and pricing is authorized to respond to this RFQ on the vendor's behalf, as confirmed by the signature below.

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

Presidio Networked Solutions, LLC
Vendor Name

Erik Hayko
Signature

58-1667655
FEIN

Erik Hayko
Signatory Printed Name

May 19, 2023
Date

Florida Digital Service
 RFQ Title: Endpoint Detection and Response Solution
 RFQ Number: DMS-22/23-155
 Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

6) ATTACHMENT B – CONTACT INFORMATION SHEET

RFQ Text:

Contact Information Sheet, containing the contacts for the Quote and the resulting ATC(s) and PO(s).

Response:

ATTACHMENT B CONTACT INFORMATION SHEET

The vendor shall provide the contact information for the Quote and a contact for the resulting ATC and PO contact in the table below.

II. Contact Information

	Contact for Quoting Purposes	Contact for the ATC and PO (if awarded)
Name:	Emily Phares	Emily Phares
Title:	Account Manager	Account Manager
Address (Line 1):	5337 Millenia Lakes Boulevard	5337 Millenia Lakes Boulevard
Address (Line 2):	Suite 300	Suite 300
City, State, Zip Code	Orlando, FL 32839	Orlando, FL 32839
Telephone (Office):	850-270-2988	850-270-2988
Telephone (Mobile):	850-524-3230	850-524-3230
Email:	ephares@presidio.com	ephares@presidio.com

Florida Digital Service
RFQ Title: Endpoint Detection and Response Solution
RFQ Number: DMS-22/23-155
Date Due: May 19, 2023, 5:00 PM EST

PRESIDIO®

7) NON-DISCLOSURE AGREEMENT

RFQ Text:

Non-Disclosure Agreement executed by the vendor.

Response:

Presidio's NDA is attached below.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Section 1. Purchase Order.

A. Composition and Priority.

The Contractor agrees to provide commodities or contractual services to the Agency within the manner and at the location specified in the Purchase Order, and any attachments to the Purchase Order. These Purchase Order Terms and Conditions, whether generic or specific, shall take precedence over any inconsistent or conflicting provision in the State of Florida, General Contract Conditions, PUR 1000. Additionally, the terms of the Purchase Order supersede the terms of any and all prior agreements with respect to this purchase.

B. Initial Term.

Unless otherwise specified, the Purchase Order begins on the date of issuance. Contractual services or commodities to be provided by the Contractor shall be completed by the date specified on the Purchase Order end date.

Section 2. Performance.

A. Performance Standards.

The Contractor agrees to perform all tasks and provide deliverables as set forth in the Statement of Work and attachments to the Purchase Order. The Agency shall be entitled at all times, upon request, to be advised as to the status of work being done by the Contractor and of the details thereof. Coordination shall be maintained by the Contractor with representatives of the Agency, or of other agencies involved in the project on behalf of the Agency.

B. Performance Deficiency.

If the Agency determines that the performance of the Contractor is unsatisfactory, the Agency may notify the Contractor of the deficiency to be corrected, which correction shall be made within a time-frame specified by the Agency. The Contractor shall provide the Agency with a corrective action plan describing how the Contractor will address all issues of contract non-performance, unacceptable performance, and failure to meet the minimum performance levels, deliverable deficiencies, or contract non-compliance. If the corrective action plan is unacceptable to the Agency, the Contractor will be assessed a non-performance retainage equivalent to 10% of the total invoice amount or as specified in the contractual documents. The retainage will be applied to the invoice for the then-current billing period. The retainage will be withheld until the Contractor resolves the deficiency. If the deficiency is subsequently resolved, the Contractor may invoice the Agency for the retained amount during the next billing period. If the Contractor is unable to resolve the deficiency, the funds retained will be forfeited.

Section 3. Payment and Fees.

A. Payment Invoicing.

The Contractor will be paid upon submission of properly certified invoice(s) to the Agency after delivery and acceptance of commodities or contractual services is

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

confirmed in writing by the Agency. Invoices shall contain detail sufficient for audit thereof and shall contain the Purchase Order and the Contractor's Federal Employer Identification Number or Social Security Number.

B. Payment Timeframe.

Section 215.422, Florida Statutes (F.S.), provides that agencies have five (5) working days to inspect and approve commodities or contractual services. Items may be tested for compliance with specifications. Items delivered not conforming to specifications may be rejected and returned at the Contractor's expense. Interest penalties for late payment are also provided for in section 215.422, F.S. A Vendor Ombudsman, whose duties include acting as an advocate for Vendors who may be experiencing problems obtaining timely payment(s) from an Agency, may be contacted at 850-413-5516, or Vendors may call the State Comptroller's Hotline at 1-800-848-3792.

C. MyFloridaMarketPlace Fees.

The following language is included pursuant to rule 60A-1.031, Florida Administrative Code:

The State of Florida, through the Department of Management Services, has instituted MyFloridaMarketPlace, a statewide eProcurement system pursuant to section 287.057(22), Florida Statutes. Payments issued by Agencies or Eligible Users to Vendors for purchases of commodities or contractual services are subject to Transaction Fees, as prescribed by rule 60A-1.031, Florida Administrative Code, or as may otherwise be established by law. Vendors shall submit monthly reports required by the rule. All reports shall be subject to audit. Failure to pay Transaction Fees or submit reports shall constitute grounds for default and exclusion from business with the State of Florida.

D. Payment Audit.

Records of costs incurred under terms of the Purchase Order shall be maintained and made available to the Agency upon request at all times during the period of the Purchase Order, and for a period of three years thereafter. Records of costs incurred shall include the Contractor's general accounting records, together with supporting documents and records of the Contractor and all subcontractors performing work, and all other records of the Contractor and subcontractors considered necessary by the Agency for audit.

E. Annual Appropriation and Travel.

Pursuant to section 287.0582, F.S., if the Purchase Order binds the State or an executive agency for the purchase of services or tangible personal property for a period in excess of one (1) fiscal year, the State of Florida's performance and obligation to pay under this contract is contingent upon an annual appropriation by the Legislature. Travel expenses are not reimbursable unless specifically authorized in writing, and shall be reimbursed only in accordance with section 112.061, F.S.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Section 4. Liability.

A. Indemnity.

To the extent permitted by Florida law, the Contractor agrees to indemnify, defend, and hold the State of Florida, its officers, employees and agents harmless from all fines, claims, assessments, suits, judgments, or damages, consequential or otherwise, including court costs and attorney's fees, arising out of any acts, actions, breaches, neglect or omissions of the Contractor, its employees, agents, subcontractors, assignees or delegates related to the Purchase Order, as well as for any determination arising out of or related to the Purchase Order, that the Contractor or Contractor's employees, agents, subcontractors, assignees or delegates are not independent contractors in relation to the Agency. The Purchase Order does not constitute a waiver of sovereign immunity or consent by the Agency or the State of Florida or its subdivisions to suit by third parties.

B. Payment for Claims.

The Contractor guarantees the payment of all just claims for materials, supplies, tools, or labor and other just claims against the Contractor or any employee, agent, subcontractor, assignee or delegate in connection with the Purchase Order.

C. Liability Insurance.

The Contractor shall maintain insurance sufficient to adequately protect the Agency from any and all liability and property damage/hazards which may result from the performance of the Purchase Order. All insurance shall be with insurers qualified and duly licensed to transact business in the State of Florida. If required by the Agency and prior to commencing any work the Contractor shall provide Certification(s) of Insurance evidencing that all appropriate coverage is in full force and showing the Agency to be an additional insured.

D. Workers' Compensation.

The Contractor shall maintain Workers' Compensation insurance as required under the Florida Workers' Compensation Law.

E. Performance Bond.

Unless otherwise prohibited by law, the Agency may require the Contractor to furnish, without additional cost to the Agency, a performance bond or irrevocable letter of credit or other form of security for the satisfactory performance of work hereunder. The Agency shall determine the type and amount of security.

Section 5. Compliance with Laws.

A. Conduct of Business.

The Contractor shall comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and authority. For example, the Contractor shall comply with Section 247A of the Immigration and Nationality Act, the

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Americans with Disabilities Act, Health Insurance Portability and Accountability Act, and all prohibitions against discrimination on the basis of race, religion, sex, creed, national origin, handicap, marital status, or veteran's status.

Pursuant to subsection 287.058(1), F.S., the provisions of subparagraphs 287.058(1)(a)-(c), and (g), F.S., are hereby incorporated by reference, to the extent applicable.

B. Lobbying.

In accordance with sections 11.062 and 216.347, F.S., the Purchase Order funds are not for the purpose of lobbying the Legislature, the judicial branch, or an Agency. Pursuant to subsection 287.058(6), F.S., the Purchase Order does not prohibit the Contractor from lobbying the executive or legislative branch concerning the scope of services, performance, term, or compensation regarding the Purchase Order, after the Purchase Order's execution and during the Purchase Order's term.

C. Gratuities.

The Contractor shall not, in connection with this or any other agreement with the State, directly or indirectly (1) offer, give, or agree to give anything of value to anyone as consideration for any State officer or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty, or (2) offer, give, or agree to give to anyone anything of value for the benefit of, or at the direction or request of, any State officer or employee.

D. Cooperation with Inspector General.

Pursuant to subsection 20.055(5), F.S., Contractor, and any subcontractor to the Contractor, understand and will comply with their duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing. Upon request of the Inspector General or any other authorized State official, the Contractor shall provide any type of information the Inspector General deems relevant to the Contractor's integrity or responsibility. Such information may include, but shall not be limited to, the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Purchase Order. The Contractor shall retain such records for three (3) years after the expiration of the Purchase Order, or the period required by the General Records Schedules maintained by the Florida Department of State (available at: <http://dos.myflorida.com/library-archives/records-management/general-records-schedules/>), whichever is longer. The Contractor agrees to reimburse the State for the reasonable costs of investigation incurred by the Inspector General or other authorized State official for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the State which results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to: salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees.

E. Public Records.

To the extent required by the Florida Public Records Act, Chapter 119, F.S., the Contractor shall maintain and allow access to public records made or received in

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

conjunction with the Purchase Order. The Purchase Order may be terminated for cause by the Agency for the Contractor's refusal to allow access to public records.

F. Communications and Confidentiality.

The Contractor agrees that it shall make no statements, press releases, or publicity releases concerning the Purchase Order or its subject matter or otherwise disclose or permit to be disclosed any of the data or other information obtained or furnished in compliance with the Purchase Order, or any particulars thereof, during the period of the Purchase Order, without first notifying the Agency's Contract Manager or the Agency's designated contact person and securing prior written consent. The Contractor shall maintain confidentiality of all confidential data, files, and records related to the services and/or commodities provided pursuant to the Purchase Order and shall comply with all state and federal laws, including, but not limited to sections 381.004, 384.29, 392.65, and 456.057, F.S. The Contractor's confidentiality procedures shall be consistent with the most recent version of the Agency's security policies, protocols, and procedures. The Contractor shall also comply with any applicable professional standards with respect to confidentiality of information.

G. Intellectual Property.

Unless specifically addressed in the Purchase Order, intellectual property rights to all property created or otherwise developed by the Contractor for the Agency will be owned by the State of Florida through the Agency at the completion of the Purchase Order. Proceeds to any Agency derived from the sale, licensing, marketing or other authorization related to any such Agency-controlled intellectual property right shall be handled in the manner specified by applicable state statute.

H. Convicted and Discriminatory Vendor Lists.

In accordance with sections 287.133 and 287.134, F.S., an entity or affiliate who is on the Convicted Vendor List or the Discriminatory Vendor List may not perform work as a contractor, supplier, subcontractor, or consultant under the Purchase Order with any Agency.

Section 6. Termination.

A. Termination for Convenience.

The Purchase Order may be terminated by the Agency in whole or in part at any time in the best interest of the Agency. If the Purchase Order is terminated before performance is completed, the Contractor shall be paid only for that work satisfactorily performed for which costs can be substantiated. Such payment, however, may not exceed an amount which is the same percentage of the Purchase Order price as the amount of work satisfactorily performed. All work in progress shall become the property of the Agency and shall be turned over promptly by the Contractor.

B. Termination for Cause.

If the Agency determines that the performance of the Contractor is not satisfactory, the Agency shall have the option of (a) immediately terminating the Purchase Order, or (b)

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

notifying the Contractor of the deficiency with a requirement that the deficiency be corrected within a specified time, otherwise the Purchase Order will be terminated at the end of such time, or (c) take other action deemed appropriate by the Agency.

Section 7. Subcontractors and Assignments.

A. Subcontractors.

The Contractor shall not subcontract any work under the Purchase Order without the prior written consent of the Agency. The Contractor is fully responsible for satisfactory completion of all subcontracted work.

B. Assignment.

The Contractor shall not sell, assign or transfer any of its rights, duties or obligations under the Purchase Order without the prior written consent of the Agency. In the event of any assignment, the Contractor remains secondarily liable for performance of the Purchase Order, unless the Agency expressly waives such secondary liability. The Agency may assign the Purchase Order with prior written notice to the Contractor.

Section 8. RESPECT and PRIDE.

A. RESPECT.

In accordance with subsection 413.036(3), F.S., if a product or service required for the performance of the Purchase Order is on the procurement list established pursuant to subsection 413.035(2), F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES THAT ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM A NONPROFIT AGENCY FOR THE BLIND OR FOR THE SEVERELY HANDICAPPED THAT IS QUALIFIED PURSUANT TO CHAPTER 413, FLORIDA STATUTES, IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 413.036(1) AND (2), FLORIDA STATUTES; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THE STATE AGENCY INsofar AS DEALINGS WITH SUCH QUALIFIED NONPROFIT AGENCY ARE CONCERNED.

Additional information about the designated nonprofit agency and the products it offers is available at <http://www.respectofflorida.org>.

B. PRIDE.

In accordance with subsection 946.515(6), F.S., if a product or service required for the performance of the Purchase Order is certified by or is available from Prison Rehabilitative Industries and Diversified Enterprises, Inc. (PRIDE) and has been approved in accordance with subsection 946.515(2), F.S., the following statement applies:

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES WHICH ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM THE CORPORATION IDENTIFIED UNDER CHAPTER 946, F.S., IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 946.515(2) AND (4), F.S.; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THIS AGENCY INsofar AS DEALINGS WITH SUCH CORPORATION ARE CONCERNED.

Additional information about PRIDE and the products it offers is available at <http://www.pride-enterprises.org>.

Section 9. Miscellaneous.

A. Independent Contractor.

The Contractor and its employees, agents, representatives, and subcontractors are not employees or agents of the Agency and are not entitled to the benefits of State of Florida employees. The Agency shall not be bound by any acts or conduct of the Contractor or its employees, agents, representatives, or subcontractors. The Contractor agrees to include this provision in all of its subcontracts under the Purchase Order.

B. Governing Law and Venue.

The laws of the State of Florida shall govern the Purchase Order. The Parties submit to the jurisdiction of the courts of the State of Florida exclusively for any legal action related to the Purchase Order. Further, the Contractor hereby waives any and all privileges and rights relating to venue it may have under Chapter 47, F.S., and any and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to those based on convenience. The Contractor hereby submits to venue in the county chosen by the Agency.

C. Waiver.

The delay or failure by the Agency to exercise or enforce any of its rights under the Purchase Order shall not constitute waiver of such rights.

D. Modification and Severability.

The Purchase Order may only be modified by a change order agreed to by the Agency and the Contractor. Should a court determine any provision of the Purchase Order is invalid, the remaining provisions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the Purchase Order did not contain the provision held to be invalid.

E. Time is of the Essence.

Time is of the essence with regard to each and every obligation of the Contractor. Each such obligation is deemed material, and a breach of any such obligation (including a breach resulting from untimely performance) is a material breach.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

F. Background Check.

The Agency may require the Contractor and its employees, agents, representatives and subcontractors to provide fingerprints and be subject to such background check as directed by the Agency. The cost of the background check(s) shall be borne by the Contractor. The Agency may require the Contractor to exclude the Contractor's employees, agents, representatives or subcontractors based on the background check results.

G. E-Verify.

In accordance with Executive Order 11-116, the Contractor agrees to utilize the U.S. Agency of Homeland Security's E-Verify system, <https://e-verify.uscis.gov/emp>, to verify the employment eligibility of all new employees hired during the term of the Purchase Order for the services specified in the Purchase Order. The Contractor shall also include a requirement in subcontracts that the subcontractor shall utilize the E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor during the Purchase Order term.

H. Commodities Logistics.

The following provisions shall apply to all Purchase Orders unless otherwise indicated in the contract documents:

- 1) All purchases are F.O.B. destination, transportation charges prepaid.
- 2) Each shipment must be shipped to the address indicated on the face of the Purchase Order and marked to the attention of the individual identified, if any. Each shipment must be labeled plainly with the Purchase Order number and must show the gross, tare, and net weight. A complete packing list must accompany each shipment. This paragraph shall also apply to any third party who ships items on behalf of the Contractor.
- 3) No extra charges shall be applied for boxing, crating, packing, or insurance.
- 4) The following delivery schedule shall apply: 8:00 AM – 4:00 PM, Monday through Friday, excluding legal holidays.
- 5) If delivery to the specified destination cannot be made on or before the specified date, notify the Agency immediately using the contact information provided in the MyFloridaMarketPlace system.
- 6) The Agency assumes no liability for merchandise shipped to other than the specified destination.
- 7) Items received in excess of quantities specified may, at Agency's option, be returned at the Contractor's expense. Substitutions are not permitted.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK



4050 Esplanade Way
Tallahassee, FL 32399-0950

Ron DeSantis, Governor
Pedro Allende, Secretary

**CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT
BETWEEN
FLORIDA DEPARTMENT OF MANAGEMENT SERVICES
AND
Presidio Networked Solutions, LLC**

This Confidentiality and Non-Disclosure Agreement (“Agreement”) is between the Florida Department of Management Services (“Department”), a state agency, and Presidio Networked Solutions, LLC (“Recipient”), referred to herein collectively as the “Parties” and individually as a “Party.”

WHEREAS, Recipient has or will enter into a Purchase Order or Agency Term Contract under Request for Quote No. DMS-22/23-155, Endpoint Detection and Response Solution (“Solution”);

WHEREAS, in furtherance of providing these services and/or commodities, Recipient may access, receive, or create Confidential Information from the Department or any third-party beneficiaries; and

WHEREAS, the Department maintains certain protections on such Confidential Information and desires to set forth the terms Recipient is required to adhere to.

NOW THEREFORE, for the mutual and valuable consideration acknowledged by both Parties, the Parties agree as follows:

1. Definitions.

- (a) **Access**: Means the ability or authorization to create, inspect, transmit, approach, instruct, communicate with, store, retrieve, or otherwise make use of any Confidential Information, regardless of type, form, or nature of storage. “Access” to a computer system or network includes local and remote access.
- (b) **Affiliates**: Any agents, affiliates, partners, subcontractors, resellers, distributors, dealers, or other entities associated with Recipient that have Access to the Confidential Data.
- (c) **Agreement-related Materials**: Materials created or provided by Recipient while performing the Agreement.
- (d) **Confidential Information**: Information that is restricted from public disclosure based on federal or State laws and regulations including, but not limited to, those related to privacy, confidentiality, security, personally identifying information, personal health, business or trade secret information, and other information exempt from state public records law. “Confidential Information” includes information disclosed, orally or otherwise, before, on, or after this Agreement effective date by the Department to Recipient, and whether or not marked, designated, or otherwise identified as “confidential.” Any information derived from Confidential Information and/or created by Recipient pursuant to this Agreement which must be restricted from public disclosure based on federal or State laws and regulations shall be considered Confidential Information subject to the restrictions set forth in this Agreement.

Specifically, Recipient will receive and may create or learn of information which include network schematics, hardware and software configurations, or encryption, or which identify detection, investigation, or response practices for suspected or confirmed IT security incidents, including suspected or confirmed breaches, the disclosure of which would facilitate unauthorized access, modification, disclosure, or destruction of information, IT resources, or information relating security, which are confidential and exempt from public disclosure pursuant to section 282.318(5), Florida Statutes (F.S.).

- (e) Customer: Agencies as defined in section 287.012, Florida Statute (F.S.), and Eligible Users as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.).
- (f) State: The State of Florida.

2. **Term and Termination.** This Agreement is effective upon signature by both Parties. This Agreement may be terminated by the Department when determined to be in the best interest of the State of Florida by providing Recipient with advance written notice.
3. **Intended Third Party Beneficiary.** Customers receiving services under the Solution are intended third party beneficiaries of this Agreement, entitled to enforce any rights hereunder for their benefit.
4. **Confidential Information Use.** Use of the Confidential Information shall be limited to the provisions set forth herein and to the extent necessary to provide the services and/or commodities. The Department retains full rights and title to all Confidential Information provided by it, and any information derived therefrom. Recipient has no ownership rights to the Confidential Information provided under this Agreement, or any information derived therefrom.
5. **Recipient Obligations.** Recipient shall: 1) maintain the confidentiality of all the Confidential Information pursuant to this Agreement, as required herein, 2) comply with all federal and State laws and regulations related to information privacy and security, and 3) ensure that any Affiliates comply with the preceding two requirements as to any Confidential Information shared with or otherwise Accessed by the Affiliate. Recipient shall take all measures necessary to protect against improper Access to and/or disclosure or theft of the Confidential Information and will ensure only those individuals performing services contemplated in this Agreement will be permitted to Access the Confidential Information. Recipient shall perform the following measures to preserve the privacy, security, confidentiality, integrity, and accessibility of the Confidential Information which includes, but is not limited to:
 - (a) Using the Confidential Information only to provide services and/or commodities as contemplated in this Agreement and not otherwise using the Confidential Information for Recipient's own benefit or the benefit of others, or in violation of any applicable laws or regulations;
 - (b) Not creating derivative works based upon the Confidential Information, copying the Confidential Information, or publishing or disclosing the Confidential Information to any individual or entity except in accordance with this Agreement;
 - (c) Implementing and maintaining protective administrative, technical, and organizational security measures appropriate to the nature of the Confidential Information to safeguard against unauthorized Access, disclosure, or theft of the Confidential Information;
 - (d) Maintaining the confidentiality of the Confidential Information under this Agreement in accordance with Department policies and procedures and applicable State and federal laws and regulations;

- (e) Storing and safeguarding the Confidential Information in a physically and electronically secure location where Access is limited to authorized persons;
- (f) Maintaining an up-to-date list of individuals who are authorized to Access the Confidential Information;
- (g) Instructing and requiring all individuals authorized to Access the Confidential Information to adhere to the confidentiality requirements set forth in this Agreement prior to being granted Access to the Confidential Information;
- (h) Not allowing, through action or inaction, any Confidential Information to be sent by any medium, transmitted, or to be Accessed outside of the United States. For the purposes of this restriction, "Access" does not include remote support sessions for devices that might contain the Confidential Information; however, during the remote support session the Department requires Recipient to escort the remote support access and maintain visibility of the actions taken during the remote support access. Requests for remote access will be submitted to the Department's Contract Manager. With approval, third parties may be granted time-limited terminal service access to information technology resources as necessary for fulfillment of related responsibilities. Remote connections are subject to detailed monitoring via two-way log reviews and the use of other tools; and
- (i) Performing all actions necessary to assist with all tasks in furtherance of the Department's efforts to comply with the obligations under Chapters 60FF and 60GG, Florida Administrative Code, as applicable.

6. Liability. By signing this Agreement, Recipient acknowledges Recipient shall be responsible and liable for the acts and omissions of any of Recipient's employees and/or the Affiliate(s) that result in a violation of this Agreement as if such acts or omissions were Recipient's acts or omissions. Recipient represents that it will enter into a written agreement with an Affiliate with Access to Confidential Information wherein it shall require the Affiliate agree to be bound by and adhere to the terms of this Agreement.

7. Notice of Breach. Recipient must notify the Department as expeditiously as practicable, but in all instances no later than within one (1) business day, in the event Recipient discovers any incident that involves, or which Recipient reasonably believes may involve, a breach of the Confidential Information which includes any unauthorized Access to or disclosure of the Confidential Information and/or which compromises the security, integrity, or confidentiality of the Confidential Information. Additionally, if the Department or Customer shares with Recipient information that is covered by section 501.171, F.S., Recipient is responsible for fulfilling all applicable requirements of section 501.171, F.S., including those that would otherwise be the responsibility of the Department or Customer. Recipient agrees to provide the Department and applicable Customers with all details associated with all breaches or suspected breaches and to work with the Department or the applicable Customer to investigate and resolve any breach, implement any necessary remedial measures, and perform all tasks to ensure full compliance with section 501.171, F.S., including, where applicable, providing any breach notifications to comply with this statutory requirement.

8. Indemnification. Recipient shall defend, indemnify, and hold harmless the Department, the Customer, and the State against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, in connection with any third-party claim, suit, action, or proceeding arising out of or resulting from a violation of any obligation set forth in this Agreement by Recipient (including its employees) or its Affiliates. The Agreement does not constitute a waiver of sovereign immunity or consent by the Department, Customers, or the State or its subdivisions to suit by third parties. The obligations of this paragraph shall survive the Agreement.

- 9. Contractual Remedies.** Recipient acknowledges that a breach of this Agreement, including disclosure of any of the Confidential Information, will cause irreparable injury to the Department or the Customer and will entitle the Department or the Customer, if applicable, to liquidated damages commensurate with the Department's or the Customer's internal staffing and administrative costs associated with addressing the breach. This will not preclude the Department or the Customer from recovering other damages it may suffer as a result of such a violation or seeking other legal remedies that may be available during or after the Agreement term, including obtaining injunctive relief against the breach or threatened breach of these Agreement terms.
- 10. Data Destruction.** Prior to the termination of this Agreement, Recipient shall assist the Department or the applicable Customer in exporting and extracting or destroying, at the Department's or the applicable Customer's direction, all information obtained from the Department or the applicable Customer by Recipient or created for the Department or the applicable Customer by Recipient pursuant to this Agreement at no cost, in a format acceptable to the Department or the applicable Customer without the need to purchase additional services and/or commodities. Additionally, when the Agreement is terminated, Recipient shall transfer to the Department, or the Customer as applicable, all such information in all its forms from the Department or the applicable Customer and shall destroy duplicate records in accordance with section 501.171(8), F.S., and, if applicable, section 119.0701, F.S. This obligation to transfer and destroy information survives the term of this Agreement.

Recipient shall adhere to established information destruction standards, such as those established by the National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization" (2014), in destroying duplicate information provided by the Department or the applicable Customer. See <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>. Recipient shall provide the Department, or the Customer as applicable, with written confirmation of destruction of Confidential Information in accordance with these standards. If Recipient is permitted by the Department or the applicable Customer to keep Confidential Information upon termination of this Agreement, Recipient shall continue to protect and maintain the confidentiality of the Confidential Information in accordance with applicable State and federal laws, rules, and regulations and such obligations set forth herein shall survive this Agreement.

- 11. Severability and Waiver.** If a court of competent jurisdiction deems any term or condition of this Agreement void or unenforceable, the other provisions are severable to that void provision, and will remain in full force and effect. However, to the fullest extent permitted by law, this Agreement shall be construed as if the scope or duration of such provision had been more narrowly drafted so as not to be invalid or unenforceable.

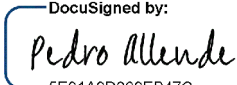
The delay or failure by the Department or the Customer to exercise or enforce any of its rights under this Agreement shall not constitute a waiver of such rights.


- 12. Governing Law and Venue.** The laws of the State of Florida govern the Agreement. The Parties submit to the jurisdiction of the courts of the State exclusively for any legal action related to the Agreement which arises during or after the Agreement term. Further, Recipient hereby waives all privileges and rights relating to venue it may have under Chapter 47, F.S., and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to, those based on convenience. Recipient hereby submits to venue in the county chosen by the Department or the applicable Customer.

13. Entire Agreement. This Agreement contains the entire understanding of the Parties regarding the matters set forth herein and shall supersede any prior negotiations or agreements, whether written or oral, with respect thereto.

IN WITNESS WHEREOF, the Parties agree to the terms and conditions of this Agreement and have duly authorized their respective representatives to sign it on the dates indicated below.

**FLORIDA DEPARTMENT
OF MANAGEMENT SERVICES**

DocuSigned by:

By: _____
5E91A9D369EB47C...
Name: Pedro Allende
Title: Secretary
Date: 6/14/2023 | 4:58 PM EDT


By: _____
Jay Staples
Name: _____
Assistant General Counsel
Title: _____
5/24/2023
Date: _____