FL [DIGITAL SERVICE]

Department of MANAGEMENT SERVICES

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

AGENCY TERM CONTRACT FOR EMAIL SECURITY DMS-22/23-161B 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-22/23-161, Email Security Solution; 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-22/23-161.

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-22/23-161;
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-22/23-161 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 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:

DocuSigned by:
Erik Hayko
E7A28D0E9E4548D...

Authorized Signature

Erik Hayko

Print Name

Senior Contracts Manager

Title

6/30/2023 | 12:17 PM EDT

Date

STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES:

DocuSigned by:
Pedro Allende
5E91A9D369EB47C...

Pedro Allende, Secretary

6/30/2023 | 12:23 PM EDT

Date

FL [DIGITAL SERVICE]

Department of MANAGEMENT SERVICES

Ron DeSantis, Florida Governor
James Grant, Florida State Chief Information Officer

Exhibit "A"

Request for Quotes (RFQ)

DMS-22/23-161

Email Security 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 email security solution that ensures the availability, integrity and authenticity of email communications by protecting against the risk of email threats.

2.0 OBJECTIVE

Pursuant to section 287.056(2), F.S., the Department intends to purchase an email security solution for use by the Department and Customers to analyze incoming email messages and detect potential threats in real-time 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 email security 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 analyze incoming email messages and detect potential threats in real-time. The Solution shall be designed to be highly effective at identifying and blocking malicious emails, while minimizing false positives (legitimate emails that are mistakenly blocked). The Department is seeking the following two major solution types of email security:

Secure Email Gateway (SEG) — for both inbound and outbound email provided as a cloud service. This service must process and filter Simple Mail Transfer Protocol (SMTP) traffic and will require organizations to change their Mail Exchange (MX) record to point to the SEG. This type of solution is traditionally used for organizations that do not use cloud provided mail services such as Microsoft Office 365 and Google Workspace.

Integrated Cloud Email Security (ICES) — cloud email providers (e.g., Microsoft and Google) provide built-in email security hygiene capabilities. ICES capabilities supplement these native features. These solutions use API access to the cloud email provider to analyze email content without the need to change the MX record.

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.

6.1.2. Content Disarm and Reconstruction

The Solution shall break down files to their discrete components in real-time and reconstruct a clean version of the email, removing anything that doesn't conform with the file type specifications, an International Organization for Standardization (ISO) standard, or company policy.

6.1.3. Multi-Source Mail Traffic Analysis

The Solution shall allow Customer configurations that have the ability to analyze emails sent and received internally and externally to and from the Customer.

6.1.4. Display Name Spoof Detection

The Solution shall detect spoofed messages based on email headers and sender names, using fuzzy matching of sender names with a predetermined list of names that are likely to be targeted.

6.1.5. Anti-Phishing Capabilities

The Solution shall provide techniques and technologies that prevent and counteract phishing attempts, unauthorized access, and theft. The Solution shall include, but not be limited to, the following capabilities:

6.1.5.1. Uniform Resource Locator (URL) and Domain Analysis: The Solution shall analyze URLs and domains in email messages to identify potential phishing attacks. This includes the ability to detect fake domains and URLs that mimic legitimate sites.

6.1.5.2. Content Analysis: The Solution shall analyze the content of email messages, including attachments and links, to identify phishing attempts. This includes the ability to detect malicious attachments and links that lead to phishing sites.

6.1.5.3. Behavioral Analysis: The Solution shall analyze the behavior of email messages, including sender behavior and user behavior, to identify potential phishing attacks. This includes the ability to detect suspicious email senders, unusual email patterns, and other anomalies that may indicate a phishing attempt.

6.1.5.4. Real-Time Threat Intelligence: The Solution shall leverage real-time threat intelligence feeds to identify and block known phishing attacks. This includes the ability to integrate with threat intelligence platforms and services to stay up-to-date with the latest threats.

6.1.6. Domain-based Message Authentication, Reporting and Conformance (DMARC) on Inbound Email

The Solution shall enforce domain-based message authentication, reporting, and conformance on inbound email traffic to protect internal users from receiving spoofed external messages.

6.1.7. 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.

6.1.8. Anomaly Detection

The Solution shall use email telemetry and analytics to detect spam and phishing, non-rule-based detection, based on metadata such as sender reputation, recipient, and envelope, email content, and communication history.

6.1.9. Lookalike Domain Detection

The Solution shall find the use of lookalike domains, also referred to as "cousin domains."

6.1.10. Remote Browser Isolation

The Solution shall reformat websites to remove security risks and provide clean rendering of the content to the client browser.

6.1.11. URL Rewriting and Time-of-Click Analysis

The Solution shall rewrite URLs to defend users by converting to non-clickable URL, replacing with plain text, or redirecting to a URL inspection service.

6.1.12. Network Sandbox

The Solution shall inspect attachments and embedded URLs in a secured sandbox and identify malware that attempts to detect being run in a virtualized sandbox environment.

6.1.13. Scalability

The Solution shall allow the mail exchange gateway to handle increased email traffic as the number of users grows over time.

6.1.14. Performance

The Solution shall allow the mail exchange gateway to process emails quickly and efficiently to ensure timely delivery.

6.1.15. Compatibility

The Solution shall have the ability to seamlessly integrate with other email systems and protocols.

6.1.16. Customization

The Solution shall offer a range of customization options to meet the specific needs of the organization and a user-friendly interface that is easy to set up and manage.

6.1.17. Administration and Configuration

The Solution shall provide robust administrative capabilities that allow organizations to manage and customize their email security policies and settings. Some of the key administrative capabilities include:

6.1.17.1. Policy Management: The Solution shall provide the ability to create and enforce email security policies that align with the Customer's security requirements. This shall include policies for anti-spam, anti-phishing, anti-malware, data loss prevention, encryption, and email archiving.

6.1.17.2. User Management: The Solution shall provide the ability to manage user accounts, roles, and permissions. This shall include the ability to create and delete user accounts, manage access rights, and configure authentication mechanisms such as single sign-on (SSO).

6.1.17.3. Configuration Management: The Solution shall provide the ability to configure email security settings such as transport rules, content filtering, quarantine settings, and notification settings. This shall include the ability to customize the security settings based on the organization's specific requirements.

6.1.17.4. Reporting and Analytics: The Solution shall provide the ability to generate detailed reports on email traffic, security incidents, policy violations, and user activity. This shall include the ability to customize and schedule reports for compliance and auditing purposes.

6.1.17.5. Integration and Automation: The Solution shall provide the ability to integrate with other security solutions and automate routine tasks such as policy updates, threat detection, and incident response. This shall include the ability to leverage APIs and connectors to integrate with third-party security solutions.

6.1.17.6. Audit and Compliance: The Solution shall provide the ability to track and log all email-related activities and events to ensure compliance with regulatory and industry standards. This shall include the ability to generate audit trails, provide access logs, and support eDiscovery requests.

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. Integration

6.1.19.1. 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.

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

6.1.19.3. The Solution shall be capable of integrating with a variety of identity and access management (IAM) systems, as well as with the applications and systems that require authentication, to meet Customer current and future needs.

6.1.19.4. 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.

6.1.19.5. 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.

6.1.20. 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.

6.1.20.1. 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.

6.1.20.2. 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. Future Integrations and Other Services

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

6.6.1.1. 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.

6.6.1.2. 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.

TABLE 1 DELIVERABLES AND FINANCIAL CONSEQUENCES			
No.	**Deliverable**	**Time Frame**	**Financial Consequences**
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.	QBRs are due 15 calendar days after the end of the quarter (January - March, April - June, July - September, and October - December). Monthly Implementation Reports are due five (5) calendar days after the end of the month. Monthly Training Reports are due five (5) calendar days after the end of the month. Monthly Service Reports are due five (5) calendar days after the end of the month. Ad hoc reports are due five (5) calendar days after the request by the Purchaser.	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 email security 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 SLA for future integrations and/or other services, if applicable, per section 6.6.1 with pricing.

e. 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 Section III for Secure Email Gateway (SEG) and/or Section IV for Integrated Cloud Email Security (ICES), 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 21.

11.0 TIMELINE

EVENT	DATE
Release of the RFQ	May 15, 2023
Pre-Quote Conference Registration Link: https://us02web.zoom.us/j/89727892578?pwd=REEwZUwrMmIyVFlDbHZVRTlzbUZHUT09	May 18, 2023, at 2:00 p.m., Eastern Time
Responses Due to the Procurement Officer, via email	May 24, 2023, by 5:00 p.m., Eastern Time
Solution Demonstrations and Quote Negotiations	May 25-30, 2023
Anticipated Award, via email	May 30, 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:**

   <u>DEPARTMENT</u>:
   CUSTODIAN OF PUBLIC RECORDS
   PHONE NUMBER: 850-487-1082
   EMAIL: PublicRecords@dms.fl.gov
   MAILING ADDRESS: 4050 ESPLANADE WAY, SUITE 160 TALLAHASSEE, FL 32399.

   <u>OTHER PURCHASER</u>:
   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 IDENITIFICATION 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 DISCRIMINATIORY, 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 <u>Screening Compliance Audits and Security Inspections</u>

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 <u>Record Retention</u>

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 20.2 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. The vendor shall provide pricing for Section III below for Secure Email Gateway (SEG) and/or Section IV below for Integrated Cloud Email Security (ICES). FL[DS] anticipates purchasing the email security 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 - Secure Email Gateway (SEG)

Initial Term Pricing (Years 1-3)		
Item No.	**Description**	**Rate Per User**
1	**<u>Initial Software Year</u>** One year of SEG software Solution as described in the RFQ per user. To include: • **implementation** • **initial training** • **initial Integration** • integration maintenance • support services	$ ___________
2	**<u>Subsequent Software Year</u>** One year of SEG software Solution as described in the RFQ per user. To include: • **ongoing training** • integration maintenance • support services	$ ___________

Optional Renewal Term Pricing (Years 4-6)		
Item No.	**Description**	**Rate Per User**
1	**Initial Software Year** One year of SEG software Solution as described in the RFQ per user. To include: • **implementation** • **initial training** • **initial Integration** • integration maintenance • support services	$ ___________
2	**Subsequent Software Year** One year of SEG software Solution as described in the RFQ per user. To include: • **ongoing training** • integration maintenance • support services	$ ___________

IV. Pricing - Integrated Cloud Email Security (ICES)

Initial Term Pricing (Years 1-3)		
Item No.	**Description**	**Rate Per User**
1	**Initial Software Year** One year of ICES software Solution as described in the RFQ per user. To include: • **implementation** • **initial training** • **initial Integration** • integration maintenance • support services	$ ___________
2	**Subsequent Software Year** One year of ICES software Solution as described in the RFQ per user. To include: • **ongoing training** • integration maintenance • support services	$ ___________

Optional Renewal Term Pricing (Years 4-6)		
Item No.	**Description**	**Rate Per User**
1	**<u>Initial Software Year</u>** One year of ICES software Solution as described in the RFQ per user. To include: • **implementation** • **initial training** • **initial Integration** • integration maintenance • support services	$ ___________
2	**<u>Subsequent Software Year</u>** One year of ICES software Solution as described in the RFQ per user. To include: • **ongoing training** • integration maintenance • support services	$ ___________

V. 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 (including implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**

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

VI. 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/or IV, and V of this attachment.

VII. 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.

VIII. Value-Added Services (Optional)

If vendors are able to offer additional services and/or commodities for email security, 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 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.

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

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 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)

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:

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.

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

Department of MANAGEMENT SERVICES
We Serve Those Who Serve Florida

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-22/23-161, Email Security 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: __________________________

PRESIDIO® | PROPOSAL RESPONSE

Florida Digital Service

Email Security Solution

Request for Quote (RFQ): DMS-22/23-161

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

Updated 6/14/2023

www.presidio.com

TABLE OF CONTENTS

TABLE OF EXHIBITS

No table of figures entries found.

1) EMAIL SECURITY SOLUTION DOCUMENTATION

Presidio is proud to partner with Cisco in response to this RFQ. Cisco Secure Email Threat Defense provides advanced protection to safeguard your inboxes. Email is still the Number 1 threat vector. Expand the scope of your defenses to detect dangerous threats and rapidly respond to and remediate new threats in real time with Cisco Secure Email. Below is a detailed description of how Cisco Secure Email meets the requirements as listed in the RFQ.

RFQ Text:

Documentation to describe the external-facing asset discovery software Solution proposed and how it meets the requirements of this RFQ.

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.

RESPONSE:

Cisco Secure Email does not directly provide for multi-tenancy. However, the Secure Gateway component provides the ability to create and manage policy for multiple domains. The ETD component provides the ability to support multiple domains within the same M365 tenant.

Further, Cisco Secure Email integrates with SecureX to provide a comprehensive view of all Cisco Secure products (Email, Endpoint, etc.) and 3rd party vendor solutions as well.

6.1.2. Content Disarm and Reconstruction

The Solution shall break down files to their discrete components in real-time and reconstruct a clean version of the email, removing anything that doesn't conform with the file type specifications, an International Organization for Standardization (ISO) standard, or company policy.

RESPONSE:

Cisco's Secure Email solution provides robust capabilities to meet the specified requirement. It includes advanced file analysis and reconstruction mechanisms that allow for real-time disassembly of email attachments into their discrete components. By leveraging advanced threat intelligence and machine learning algorithms, the solution can identify and remove any elements within the email that do not conform to the specified file type specifications, ISO standards, or your organization's policies.

Here's how Cisco Secure Email addresses this criterion:

Real-time Disassembly: Cisco's solution employs cutting-edge technologies to instantly break down email attachments into their individual components. This process enables deep visibility and analysis of each file's content, regardless of its format or complexity.

Content Reconstruction: After disassembling the files, Cisco Secure Email reconstructs a clean and sanitized version of the email by removing any non-compliant elements. This ensures that only legitimate and safe content is delivered to end users, mitigating potential threats and reducing the risk of data breaches.

File Type Specifications: Cisco's solution leverages a comprehensive database of file type specifications, allowing it to accurately identify the intended format of each attachment. This capability ensures that files are analyzed and processed according to their designated file types, preventing disguised or malicious files from bypassing security measures.

International Organization for Standardization (ISO) Standards: Cisco Secure Email aligns with ISO standards, which serve as global benchmarks for data security and management. The solution adheres to ISO standards relevant to email file formats and applies the necessary controls and policies to ensure compliance.

Company Policy Compliance:

The solution can be configured to enforce your organization's specific email security policies. It allows you to define custom rules and regulations regarding file types, content filtering, and acceptable usage. Cisco Secure Email actively enforces these policies, removing any elements that violate the established rules and keeping your email environment secure and compliant.

In summary, Cisco's Secure Email solution excels in breaking down files into their discrete components, ensuring compliance with file type specifications, ISO standards, and your company's policies. By combining real-time analysis, content reconstruction, and policy enforcement, it provides robust protection against email-based threats while maintaining a high level of data integrity and compliance.

6.1.3. Multi-Source Mail Traffic Analysis

The Solution shall allow Customer configurations that have the ability to analyze emails sent and received internally and externally to and from the Customer.

RESPONSE:

Cisco's Secure Email solution offers extensive configuration options that allow customers to analyze both internal and external emails sent and received by the organization. With this solution, you can implement comprehensive email monitoring and analysis capabilities to ensure the security of all email communication within your network perimeter. Here's how Cisco Secure Email addresses this criterion:

Internal Email Analysis: The solution provides the capability to inspect and analyze emails exchanged between users within your organization. It allows you to define rules and policies for internal email traffic, including content filtering, data loss prevention (DLP), and threat detection. This ensures that potentially harmful or sensitive content is identified and appropriate actions are taken, such as blocking, quarantining, or alerting.

External Email Analysis: Cisco Secure Email extends its analysis capabilities to emails exchanged with external entities. It employs various security mechanisms such as anti-malware scanning, spam filtering, URL reputation checks, and advanced threat intelligence to protect against external threats. The solution enables you to configure policies and rules to handle incoming and outgoing emails based on your organization's security requirements.

Customized Configurations: The solution offers a flexible and customizable configuration framework that empowers customers to define specific analysis and monitoring settings according to their unique needs. You can establish granular policies based on sender, recipient, subject, attachment types, content keywords, and other relevant criteria. This flexibility allows you to tailor the solution to match your organization's email security objectives and compliance requirements.

Data Loss Prevention (DLP): Cisco Secure Email includes robust DLP capabilities to prevent the unauthorized disclosure of sensitive information through email. You can configure DLP policies to identify and block outbound emails that contain confidential data, such as personally identifiable information (PII), financial data, or intellectual property. This helps maintain compliance with regulatory standards and safeguards your organization's critical information.

Reporting and Analytics: The solution provides comprehensive reporting and analytics features that enable you to gain insights into email traffic patterns, security events, and policy violations. You can monitor email activity, track trends, and generate customized reports to assess the effectiveness of your email security measures. This visibility allows you to identify potential vulnerabilities, make informed decisions, and continuously enhance your email security posture.

In summary, Cisco's Secure Email solution empowers customers to configure and analyze both internal and external emails sent and received by the organization. By leveraging customizable settings, DLP capabilities, and robust reporting, the solution ensures comprehensive email security, mitigates risks, and enables proactive threat detection and response.

6.1.4. Display Name Spoof Detection

The Solution shall detect spoofed messages based on email headers and sender names, using fuzzy matching of sender names with a predetermined list of names that are likely to be targeted.

RESPONSE:

Cisco's Secure Email solution offers robust capabilities to detect spoofed messages by analyzing email headers and sender names, leveraging fuzzy matching techniques with a predetermined list of names that are commonly targeted. This helps identify and prevent phishing attacks and email spoofing attempts. Here's how Cisco Secure Email addresses this criterion:

Email Header Analysis: The solution thoroughly examines the email headers, which contain essential metadata and routing information, to identify any suspicious indicators of spoofing. It analyzes fields such as "From," "Reply-To," and "Return-Path" to detect inconsistencies, abnormalities, or signs of manipulation that are commonly associated with spoofed messages.

Sender Name Fuzzy Matching: Cisco Secure Email employs fuzzy matching algorithms to compare the sender names with a predetermined list of names that are likely to be targeted in spoofing attacks. Fuzzy matching allows for variations and slight deviations in spelling or formatting, ensuring effective detection even when attackers attempt to obfuscate the sender's identity.

Targeted Name List: The solution maintains a comprehensive list of names that are frequently used or impersonated in spoofed email campaigns. This list includes commonly targeted individuals or high-profile entities within your organization. By comparing sender names against this list, Cisco Secure Email can identify potential spoofing attempts and trigger appropriate security actions or alerts.

Threat Intelligence Integration: Cisco's solution leverages threat intelligence feeds and continuously updated databases to enhance its detection capabilities. These resources include information about known phishing campaigns, malicious sender domains, and patterns associated with email spoofing. By integrating this intelligence, the solution can proactively identify emerging threats and patterns, improving its ability to detect spoofed messages effectively.

Policy Enforcement and Response: Once a spoofed message is identified, Cisco Secure Email enables you to define and enforce policies to handle such messages. You can configure actions such as blocking, quarantining, or flagging suspicious emails to protect your users from falling victim to phishing attacks. Additionally, the solution can generate alerts or notifications to security teams, allowing for swift incident response and investigation.

In summary, Cisco's Secure Email solution employs advanced techniques like email header analysis and sender name fuzzy matching to detect and prevent spoofed messages. By utilizing a targeted name list, threat intelligence integration, and policy enforcement capabilities, the solution enhances your organization's defenses against phishing attacks and email spoofing attempts. It helps safeguard your users, sensitive information, and reputation by proactively identifying and mitigating the risks associated with spoofed messages.

6.1.5. Anti-Phishing Capabilities

The Solution shall provide techniques and technologies that prevent and counteract phishing attempts, unauthorized access, and theft. The Solution shall include, but not be limited to, the following capabilities:

6.1.5.1.

Uniform Resource Locator (URL) and Domain Analysis: The Solution shall analyze URLs and domains in email messages to identify potential phishing attacks. This includes the ability to detect fake domains and URLs that mimic legitimate sites.

RESPONSE:

Cisco's Secure Email solution offers robust techniques and technologies to prevent and counteract phishing attempts, unauthorized access, and theft. It includes advanced capabilities, such as URL and domain analysis, to identify and mitigate potential phishing attacks. Here's how Cisco Secure Email addresses this specific requirement:

URL and Domain Analysis: Cisco's solution employs sophisticated algorithms to analyze URLs and domains present in email messages. It thoroughly inspects links to identify potential phishing attempts by comparing them against known malicious URLs and domain reputation databases.

This analysis helps identify URLs that lead to fake websites or mimic legitimate sites, protecting users from accessing malicious content.

Phishing URL Detection: Cisco Secure Email leverages threat intelligence feeds, machine learning, and behavior analysis to detect and block phishing URLs in real-time. The solution identifies characteristics and patterns associated with phishing attacks, including domain spoofing, typo squatting, and deceptive URL structures. By utilizing a combination of static and dynamic analysis techniques, it accurately identifies and prevents users from accessing malicious links.

Reputation and URL Categorization: The solution maintains an extensive database of known malicious URLs and domains. It performs reputation checks on URLs and domains in real-time against this database, as well as reputable URL categorization services. By assessing the reputation and categorization of URLs, Cisco Secure Email can determine the legitimacy of links and take appropriate actions based on policy settings, such as blocking, quarantining, or redirecting suspicious URLs.

Link Protection and Rewriting: Cisco's solution offers link protection features that rewrite URLs within email messages. It replaces original URLs with safe, sandboxed, or scanned equivalents, ensuring that users are directed to a secure environment before accessing potentially dangerous content. This approach provides an additional layer of protection by preventing users from inadvertently clicking on malicious links, even if the initial analysis might not have identified them as threats.

Security Awareness Training Integration: Cisco Secure Email can be integrated with security awareness training platforms to further educate users about phishing threats and safe browsing practices. This integration enables the solution to combine technical defenses with user education, reinforcing a comprehensive defense against phishing attacks and unauthorized access attempts.

In summary, Cisco's Secure Email solution offers robust capabilities to prevent and counteract phishing attempts, unauthorized access, and theft. Through URL and domain analysis, reputation checks, link protection, and integration with security awareness training, the solution enhances your organization's defenses against phishing attacks. It helps safeguard your users, data, and network infrastructure by proactively detecting and mitigating the risks associated with fake domains and URLs.

6.1.5.2.

Content Analysis: The Solution shall analyze the content of email messages, including attachments and links, to identify phishing attempts. This includes the ability to detect malicious attachments and links that lead to phishing sites.

RESPONSE:

Cisco's Secure Email solution offers powerful techniques and technologies to prevent and counteract phishing attempts, unauthorized access, and theft. It includes comprehensive content analysis capabilities to identify and mitigate phishing attempts within email messages, including attachments and links. Here's how Cisco Secure Email addresses this specific requirement:

Content Inspection: Cisco's solution thoroughly inspects the content of email messages, including attachments and embedded links. It employs advanced algorithms and machine learning techniques to analyze the characteristics, behavior, and patterns associated with phishing attempts. By examining the content, it can identify malicious elements and take appropriate actions to mitigate the risks.

Attachment Analysis: Cisco Secure Email applies robust scanning mechanisms to analyze email attachments in real-time. It leverages multiple layers of protection, including signature-based detection, heuristic analysis, and sandboxing. These techniques enable the solution to detect and block malicious attachments, including those carrying malware, ransomware, or other types of malicious code.

Link Analysis: The solution examines links embedded within email messages to identify potential phishing attempts. It performs real-time URL and domain analysis, comparing them against known malicious URLs and domain reputation databases. By utilizing advanced threat intelligence, behavioral analysis, and machine learning, Cisco Secure Email can accurately detect and block links that lead to phishing sites or malicious content.

Threat Intelligence Integration: Cisco's solution integrates with a vast array of threat intelligence sources and databases. It continuously updates its knowledge base with the latest information about emerging phishing campaigns, malicious URLs, and email-based threats. By leveraging this intelligence, the solution enhances its ability to identify and counteract new and evolving phishing attempts.

Machine Learning and Behavioral Analysis: Cisco Secure Email utilizes machine learning algorithms and behavioral analysis techniques to identify patterns and anomalies associated with phishing attempts. By continuously analyzing the behavior of email messages, attachments, and links, the solution can detect subtle indicators of phishing and unauthorized access. This proactive approach helps identify sophisticated phishing attacks that may evade traditional signature-based detection.

In summary, Cisco's Secure Email solution provides robust content analysis capabilities to prevent and counteract phishing attempts, unauthorized access, and theft. By inspecting email content, attachments, and links, and utilizing advanced techniques such as attachment analysis, link analysis, threat intelligence integration, machine learning, and behavioral analysis, the solution enhances your organization's defenses against phishing attacks. It helps protect your users, data, and network infrastructure by proactively identifying and mitigating the risks associated with malicious attachments and phishing links.

6.1.5.3.

Behavioral Analysis: The Solution shall analyze the behavior of email messages, including sender behavior and user behavior, to identify potential phishing attacks. This includes the ability to detect suspicious email senders, unusual email patterns, and other anomalies that may indicate a phishing attempt.

RESPONSE:

Cisco's Secure Email solution offers robust behavioral analysis capabilities to analyze the behavior of email messages, including sender behavior and user behavior, in order to identify potential phishing attacks. The solution leverages advanced techniques and algorithms to detect suspicious email senders, unusual email patterns, and other anomalies that may indicate phishing attempts. Here's how Cisco Secure Email addresses this specific requirement:

Sender Behavior Analysis: Cisco's solution examines the behavior of email senders to identify suspicious or malicious activity. It analyzes various attributes such as sender reputation, historical sending patterns, and authentication mechanisms (e.g., SPF, DKIM, DMARC) to determine the legitimacy and trustworthiness of the sender. Deviations from normal behavior or indications of spoofing are flagged as potential phishing attempts.

User Behavior Analysis: The solution tracks user behavior within the email system to identify anomalies that may indicate a phishing attempt. It analyzes patterns such as unusual email forwarding, abnormal login locations or times, sudden spikes in sent messages, or bulk actions that may suggest a compromised account or malicious activity. By comparing user behavior against established baselines, the solution can quickly detect and alert on suspicious behavior.

Anomaly Detection: Cisco Secure Email employs advanced anomaly detection techniques to identify deviations from normal email behavior. It utilizes machine learning algorithms to establish patterns and baselines of legitimate email behavior, including sender behavior and user behavior.

Any deviations or anomalies, such as unexpected changes in sending patterns or unusual email content, are flagged as potential indicators of phishing attempts.

Threat Intelligence Integration: The solution integrates with threat intelligence feeds and databases to enhance its behavioral analysis capabilities. It leverages the latest information about known phishing campaigns, malicious sender profiles, and suspicious email patterns. By incorporating this intelligence, Cisco Secure Email can proactively detect and block phishing attempts based on behavioral indicators observed across different organizations.

Policy Enforcement and Response: Once potential phishing attempts are identified through behavioral analysis, the solution allows you to define and enforce policies to handle such messages. Policies can include actions such as blocking, quarantining, or alerting on suspicious emails. Additionally, the solution can generate real-time notifications or alerts to security teams, enabling swift incident response and investigation.

In summary, Cisco's Secure Email solution includes robust behavioral analysis capabilities to detect potential phishing attacks. By analyzing sender behavior, user behavior, and employing advanced anomaly detection techniques, the solution enhances your organization's ability to identify and mitigate phishing attempts. It helps safeguard your users, data, and network infrastructure by proactively detecting suspicious email senders, unusual email patterns, and other anomalies that may indicate phishing activity.

6.1.5.4.

Real-Time Threat Intelligence: The Solution shall leverage real- time threat intelligence feeds to identify and block known phishing attacks. This includes the ability to integrate with threat intelligence platforms and services to stay up-to-date with the latest threats.

RESPONSE:

Cisco's Secure Email solution leverages real-time threat intelligence feeds to effectively identify and block known phishing attacks. The solution is designed to integrate with threat intelligence platforms and services, ensuring it stays up-to-date with the latest threats. Here's how Cisco Secure Email addresses this specific requirement:

Real-Time Threat Intelligence Integration: Cisco's solution integrates with reputable threat intelligence platforms and services to receive real-time updates about emerging phishing attacks and evolving threat landscapes. By connecting with these sources, Cisco Secure Email ensures that it has access to the most current information and can quickly adapt its defenses to counter new and emerging threats.

Continuous Updates and Feeds: The solution maintains a comprehensive and constantly updated database of known phishing attack indicators, malicious domains, suspicious IP addresses, and other threat intelligence data. It regularly receives threat feeds, ensuring that the latest threat intelligence is promptly incorporated into its security mechanisms. This allows Cisco Secure Email to proactively identify and block known phishing attacks in real-time.

Dynamic Analysis and Reputation Checks: Cisco's solution applies real-time threat intelligence to perform dynamic analysis and reputation checks on email content, attachments, links, and sender profiles. By comparing the observed elements against known threat indicators and patterns, the solution can identify and block malicious emails associated with known phishing campaigns or compromised sources.

Collaborative Protection: Cisco Secure Email fosters collaborative protection by sharing threat intelligence with other security solutions and platforms within the Cisco security ecosystem. This collaborative approach ensures that organizations benefit from a broader threat intelligence network, where collective knowledge and insights help identify and block sophisticated phishing attacks across multiple environments.

Machine Learning and Behavioral Analysis: The solution utilizes machine learning algorithms and behavioral analysis to identify new and emerging phishing attacks that may not be explicitly identified in threat intelligence feeds. By continuously monitoring email behavior, content, and user interactions, Cisco Secure Email can detect patterns and anomalies indicative of phishing attempts, even if they are not yet listed in threat intelligence feeds.

In summary, Cisco's Secure Email solution leverages real-time threat intelligence feeds to identify and block known phishing attacks. By integrating with threat intelligence platforms, receiving continuous updates, and incorporating dynamic analysis, reputation checks, machine learning, and behavioral analysis, the solution ensures that it remains up-to-date and capable of detecting and mitigating the latest phishing threats. It provides robust protection against known phishing attacks while also proactively identifying emerging threats for effective email security.

6.1.6.

Domain-based Message Authentication, Reporting and Conformance (DMARC) on Inbound Email

The Solution shall enforce domain-based message authentication, reporting, and conformance on inbound email traffic to protect internal users from receiving spoofed external messages.

RESPONSE:

Cisco's Secure Email solution provides robust capabilities to enforce domain-based message authentication, reporting, and conformance (DMARC) on inbound email traffic. This ensures the protection of internal users from receiving spoofed external messages. Here's how Cisco Secure Email addresses this specific requirement:

DMARC Implementation: Cisco's solution supports DMARC, an email authentication protocol that helps prevent domain spoofing and email impersonation. It enables you to define DMARC policies for your domains, specifying how to handle emails that fail authentication checks. By enforcing DMARC, the solution protects internal users from receiving emails that appear to be from trusted external domains but are, in fact, spoofed or malicious.

Authentication Mechanisms: Cisco Secure Email incorporates authentication mechanisms such as Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to validate the authenticity of incoming email messages. SPF checks the sender's IP address against the authorized list of sending servers for a specific domain, while DKIM verifies the integrity of the email's contents using cryptographic signatures. These mechanisms enhance the DMARC enforcement process, ensuring that only legitimate emails from authenticated sources are delivered to internal users.

Reporting and Monitoring: The solution provides comprehensive reporting and monitoring capabilities for DMARC implementation. It generates DMARC reports that provide insights into the alignment and authentication status of incoming email traffic. These reports help you identify any attempted domain spoofing or email impersonation, allowing you to take appropriate actions to protect your internal users.

Policy Enforcement: Cisco Secure Email enables you to define and enforce DMARC policies tailored to your organization's needs. You can set policies to quarantine or reject emails that fail DMARC checks, providing granular control over the handling of potentially spoofed messages. By enforcing DMARC policies, the solution helps prevent fraudulent emails from reaching your internal users and reduces the risk of falling victim to phishing or impersonation attacks.

Education and Awareness: Alongside DMARC enforcement, Cisco's solution supports user education and awareness initiatives to help internal users recognize and report suspicious emails.

By combining DMARC enforcement with security awareness training, you can empower your users to be vigilant and report any potentially spoofed emails they receive, further strengthening your organization's defenses against email-based threats.

In summary, Cisco's Secure Email solution enforces domain-based message authentication, reporting, and conformance (DMARC) on inbound email traffic to protect internal users from receiving spoofed external messages. By implementing DMARC, utilizing authentication mechanisms, providing reporting capabilities, enabling policy enforcement, and promoting user education, the solution helps ensure the authenticity of incoming emails, mitigating the risk of domain spoofing and email impersonation.

6.1.7. 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's Secure Email solution offers user-friendly interfaces with intuitive designs to facilitate user engagement and simplify the management of email security. Additionally, Cisco provides clear documentation and comprehensive support resources to ensure users can effectively utilize the solution. Here's how Cisco Secure Email addresses this requirement:

User-Friendly Interfaces: Cisco's solution features user-friendly interfaces designed to provide a seamless experience for administrators and end-users. The interfaces are designed with intuitive layouts, clear navigation, and logically organized features, making it easy for users to understand and access the necessary functionality. The interfaces prioritize usability, enabling users to quickly configure settings, review security reports, and perform common tasks without extensive training or technical expertise.

Intuitive Design: Cisco Secure Email incorporates intuitive design principles to enhance user engagement. The solution employs consistent visual elements, icons, and terminology, ensuring a familiar and intuitive experience across different features and modules. The design promotes user adoption and reduces the learning curve, allowing users to quickly become proficient in managing email security.

Clear Documentation: Cisco provides clear documentation that serves as a comprehensive guide for deploying, configuring, and managing the Secure Email solution. The documentation includes step-by-step instructions, best practices, and troubleshooting guides, ensuring users have the necessary resources to understand and effectively utilize the solution. It covers various aspects, from initial setup to advanced configuration options, and helps users maximize the benefits of the solution.

Support Resources: Cisco offers robust support resources to assist users in using the Secure Email solution. This includes online knowledge bases, community forums, and technical support channels where users can access additional information, seek assistance, and collaborate with experts and peers. The support resources aim to address any questions or issues promptly, ensuring users have the necessary support to overcome challenges and optimize their use of the solution.

Training and Education: Cisco provides training programs and educational resources to empower users with in-depth knowledge and skills to effectively utilize the Secure Email solution. These training programs can be customized to cater to different user roles and proficiency levels. Through training, users gain a deeper understanding of the solution's features, best practices for email security, and how to respond to emerging threats.

In summary, Cisco's Secure Email solution offers user-friendly interfaces with intuitive designs to enhance user engagement and simplify email security management. The solution is supported by clear documentation, comprehensive support resources, and training programs, ensuring users have the necessary guidance and assistance to utilize the solution effectively. This holistic approach promotes user adoption, confidence, and productivity in managing email security.

6.1.8. Anomaly Detection

The Solution shall use email telemetry and analytics to detect spam and phishing, non-rule-based detection, based on metadata such as sender reputation, recipient, and envelope, email content, and communication history.

RESPONSE:

Cisco's Secure Email solution utilizes email telemetry and analytics to effectively detect spam and phishing attacks. The solution incorporates non-rule-based detection techniques that leverage various metadata, email content, and communication history to identify suspicious and malicious emails. Here's how Cisco Secure Email addresses this requirement:

Email Telemetry and Metadata Analysis: Cisco's solution leverages email telemetry data and metadata, including sender reputation, recipient information, and envelope details, to identify potential spam and phishing attacks. By analyzing this metadata, the solution can detect anomalies, such as suspicious sender behavior or mismatches between the sender and recipient, to flag potentially malicious emails.

Content Analysis: Cisco Secure Email employs advanced content analysis techniques to scrutinize the email content for signs of spam and phishing. This includes analyzing email body, subject lines, attachments, and embedded links. By examining the content, the solution can detect phishing indicators, suspicious keywords, known spam patterns, and other malicious elements to accurately identify and block spam and phishing attempts.

Communication History: The solution takes into account the communication history between sender and recipient to assess the legitimacy of an email. By analyzing past interactions, patterns of communication, and email behavior, Cisco Secure Email can identify anomalies that may indicate a phishing attempt or a compromised account. Unusual communication patterns or sudden changes in the frequency or nature of emails can trigger alerts for further investigation.

Machine Learning and Behavioral Analysis: Cisco's solution employs machine learning algorithms and behavioral analysis techniques to identify patterns and anomalies associated with spam and phishing attacks. By continuously analyzing email telemetry, metadata, content, and user behavior, the solution can detect subtle indicators of spam and phishing attempts, even when traditional rule-based detection mechanisms may not capture emerging threats.

Threat Intelligence Integration: Cisco Secure Email integrates with threat intelligence feeds and databases to enhance its spam and phishing detection capabilities. It leverages up-to-date information about known spam campaigns, malicious senders, and phishing indicators. By incorporating this intelligence, the solution enhances its ability to proactively identify and block new and emerging spam and phishing attacks.

In summary, Cisco's Secure Email solution utilizes email telemetry, analytics, and advanced detection techniques to detect spam and phishing attacks. By analyzing metadata, email content, communication history, and leveraging machine learning and threat intelligence integration, the solution enhances your organization's ability to identify and block suspicious and malicious emails. It provides robust protection against spam and phishing, mitigating the risks associated with these threats.

6.1.9. Lookalike Domain Detection

The Solution shall find the use of lookalike domains, also referred to as "cousin domains."

RESPONSE:

Cisco's Secure Email solution includes features to detect and mitigate the use of lookalike domains, commonly known as "cousin domains," as part of its comprehensive email security capabilities. The solution employs techniques to identify domains that closely resemble legitimate domains, aiming to prevent phishing attacks and domain spoofing. Here's how Cisco Secure Email addresses this requirement:

Domain Similarity Analysis: Cisco's solution incorporates domain similarity analysis to identify lookalike domains. It compares incoming email domains with known legitimate domains, looking for similarities in spelling, structure, or other attributes that may indicate an attempt to deceive users through domain spoofing. By detecting such lookalike domains, the solution helps prevent users from interacting with malicious or deceptive websites.

Pattern Recognition: The solution utilizes advanced pattern recognition algorithms to identify domain names that closely resemble legitimate domains. It considers variations in character placement, character substitution, or the inclusion of additional characters to create deceptive domain names. By recognizing these patterns, Cisco Secure Email can flag potentially malicious emails originating from cousin domains.

Threat Intelligence Integration: Cisco Secure Email integrates with threat intelligence feeds and databases that track known instances of cousin domains used in phishing attacks. By leveraging this intelligence, the solution strengthens its ability to identify and block emails associated with such deceptive domains. Continuous updates from threat intelligence sources ensure that the solution remains up-to-date in detecting emerging threats related to lookalike domains.

Machine Learning and Behavioral Analysis: The solution utilizes machine learning and behavioral analysis techniques to detect patterns and anomalies associated with the use of lookalike domains. By analyzing historical data and user behavior, the solution can identify instances where users are receiving emails from unfamiliar or suspicious domains that closely resemble legitimate domains. This proactive approach helps protect users from falling victim to phishing attacks using cousin domains.

Real-Time Domain Reputation Checks: Cisco Secure Email performs real-time reputation checks on incoming email domains to assess their legitimacy and potential association with lookalike or cousin domains. By integrating domain reputation data and utilizing real-time analysis, the solution can identify and block emails from domains that are known or suspected to be involved in phishing activities.

In summary, Cisco's Secure Email solution includes features to detect and mitigate the use of lookalike domains or cousin domains. By employing domain similarity analysis, pattern recognition, threat intelligence integration, machine learning, behavioral analysis, and real-time reputation checks, the solution enhances your organization's defenses against phishing attacks leveraging deceptive domain names. It helps protect users by preventing them from interacting with emails originating from malicious or deceptive lookalike domains.

6.1.10. Remote Browser Isolation

The Solution shall reformat websites to remove security risks and provide clean rendering of the content to the client browser.

RESPONSE:

Cisco's Secure Email solution focuses on email security rather than web content rendering. While it doesn't directly reformat websites, it provides robust email security features to protect against email-based threats. These features include anti-malware scanning, spam filtering, phishing detection, and link protection. However, web content reformatting and rendering fall under the scope of web security solutions rather than email security.

To ensure a secure browsing experience and clean rendering of web content, organizations typically employ web security solutions such as web application firewalls (WAFs) or secure web gateways (SWGs). These solutions specialize in scanning and filtering web traffic, analyzing website code for potential security risks, and providing secure access to web content.

If your requirement involves secure web content rendering, I recommend considering web security solutions such as WAFs or SWGs. These solutions can help mitigate security risks and provide secure access to web content, ensuring a safe browsing experience for users. Cisco offers products like Cisco Umbrella Secure Internet Gateway that provide web security features to meet these requirements.

6.1.11. URL Rewriting and Time-of-Click Analysis

The Solution shall rewrite URLs to defend users by converting to non-clickable URL, replacing with plain text, or redirecting to a URL inspection service.

RESPONSE:

Cisco's Secure Email solution offers URL rewriting capabilities to defend users against potential security risks associated with malicious URLs. The solution provides multiple techniques to enhance user protection, including converting URLs to non-clickable formats, replacing them with plain text, or redirecting them to a URL inspection service. Here's how Cisco Secure Email addresses this requirement:

Non-Clickable URL Conversion: Cisco's solution can convert URLs within email messages to non-clickable formats. This prevents users from inadvertently clicking on potentially malicious links by removing the hyperlink functionality. Instead, the URLs are displayed as plain text that users can copy and paste into their browsers if they choose to access the corresponding web content.

Plain Text URL Replacement: Cisco Secure Email offers the option to replace URLs with plain text alternatives. This approach maintains the readability of the email content while removing the direct clickability of the URLs. By replacing URLs with plain text, users can visually identify the URL without the risk of accidentally activating the link.

URL Redirection to Inspection Service: The solution can also redirect suspicious URLs to a URL inspection service. When users click on a potentially malicious link, Cisco Secure Email intercepts the request and redirects it to an inspection service that assesses the URL for potential threats. This process provides an additional layer of protection by analyzing the URL in real-time before allowing the user to access the web content.

These URL rewriting techniques aim to enhance user security by mitigating the risk of users interacting with malicious or suspicious URLs within email messages. By converting URLs to non-clickable formats, replacing them with plain text, or redirecting them to inspection services, Cisco Secure Email helps protect users from inadvertently visiting malicious websites or falling victim to phishing or malware attacks.

It's important to note that the specific URL rewriting capabilities and options may vary based on the configuration and customization of Cisco's Secure Email solution.

6.1.12. Network Sandbox

The Solution shall inspect attachments and embedded URLs in a secured sandbox and identify malware that attempts to detect being run in a virtualized sandbox environment.

RESPONSE:

Cisco's Secure Email solution provides robust attachment and URL inspection capabilities in a secure sandbox environment. The solution utilizes advanced techniques to detect and analyze malware, including those designed to evade detection in virtualized sandbox environments. Here's how Cisco Secure Email addresses this requirement:

Secure Sandbox Environment: Cisco's solution employs a secure sandbox environment to isolate and analyze attachments and embedded URLs. This sandbox provides a controlled execution environment where potentially malicious files and URLs can be safely executed and observed. By isolating these elements, the solution mitigates the risk of malware spreading to the user's environment.

Malware Detection: Within the sandbox environment, Cisco Secure Email employs a combination of static and dynamic analysis techniques to detect and identify malware. It assesses file behavior, code execution, and network communication patterns to identify malicious activities or indicators. This multi-layered approach enhances the detection capabilities and increases the likelihood of identifying malware that may attempt to detect sandbox environments.

Evasion Techniques Detection: The solution is equipped with advanced techniques to detect and counteract evasion techniques used by malware to identify virtualized sandbox environments. It leverages behavior analysis, code obfuscation detection, and anti-evasion mechanisms to identify and neutralize attempts by malware to evade detection within the sandbox. These techniques help ensure the thorough inspection and accurate detection of malware.

Threat Intelligence Integration: Cisco Secure Email integrates with threat intelligence feeds and databases to enhance its malware detection capabilities. It continuously updates its knowledge base with the latest information about known malware strains, behavior patterns, and emerging threats. By leveraging this intelligence, the solution can proactively detect and block malware, even those designed to evade virtualized sandbox environments.

Post-Detection Actions: After analyzing attachments and embedded URLs in the sandbox, Cisco Secure Email takes appropriate actions based on the identified threats. This may include blocking or quarantining malicious files, preventing users from accessing malicious URLs, and generating alerts or notifications to security teams for further investigation and response.

In summary, Cisco's Secure Email solution inspects attachments and embedded URLs in a secure sandbox environment and employs advanced techniques to detect malware, including those designed to evade detection in virtualized sandbox environments. By utilizing secure sandboxes, multi-layered analysis, anti-evasion mechanisms, threat intelligence integration, and appropriate post-detection actions, the solution enhances your organization's ability to identify and mitigate malware threats within email attachments and URLs.

6.1.13. Scalability

The Solution shall allow the mail exchange gateway to handle increased email traffic as the number of users grows over time.

RESPONSE:

Cisco's Secure Email solution is designed to scale and handle increased email traffic as the number of users grows over time. The solution offers scalability and capacity management features to ensure that the mail exchange gateway can accommodate growing email volumes. Here's how Cisco Secure Email addresses this requirement:

Scalability: Cisco's solution is built to scale horizontally and vertically, allowing it to handle increased email traffic as the number of users grows. It can handle high email volumes by leveraging distributed architecture and load balancing mechanisms. This ensures that the mail exchange gateway can efficiently process incoming and outgoing emails, even during peak periods or as the user base expands.

Load Balancing: Cisco Secure Email supports load balancing techniques to distribute email traffic across multiple gateway instances. By distributing the load, the solution optimizes resource utilization and ensures that email traffic is evenly distributed, preventing bottlenecks and maintaining performance even with increasing user counts.

Capacity Planning: The solution provides capacity planning capabilities to help organizations effectively manage and scale their email infrastructure. It offers visibility into email traffic patterns, performance metrics, and resource utilization. This information can be used to analyze current usage trends and plan for future growth, ensuring that the mail exchange gateway is properly provisioned to handle increased email traffic.

Elasticity: Cisco's solution leverages cloud-based infrastructure or on-premises deployments with flexible resource allocation. This allows organizations to scale the mail exchange gateway up or down based on demand. The solution can dynamically allocate resources to accommodate spikes in email traffic and ensure optimal performance during periods of increased user activity.

High Availability: Cisco Secure Email supports high availability configurations to ensure continuous operation and resilience against hardware or network failures. By implementing redundant components and failover mechanisms, the solution maintains email flow and mitigates the impact of potential disruptions, allowing for uninterrupted email service as the user base grows.

In summary, Cisco's Secure Email solution provides scalability, load balancing, capacity planning, elasticity, and high availability features to handle increased email traffic as the number of users grows over time. By leveraging distributed architecture, load balancing mechanisms, capacity planning insights, and flexible resource allocation, the solution ensures optimal performance and uninterrupted email service as your organization's email traffic expands.

6.1.14. Performance

The Solution shall allow the mail exchange gateway to process emails quickly and efficiently to ensure timely delivery.

RESPONSE:

Cisco's Secure Email solution is designed to process emails quickly and efficiently, ensuring timely delivery of messages. The solution incorporates various performance optimization features to streamline email processing and minimize any potential delays. Here's how Cisco Secure Email addresses this requirement:

Advanced Email Processing: Cisco's solution employs advanced email processing techniques to handle incoming and outgoing messages efficiently. It optimizes the processing pipeline, leveraging techniques such as parallel processing and optimized algorithms to minimize processing time and ensure swift delivery of emails.

Robust Infrastructure: The solution is built on a robust infrastructure designed to handle high email volumes. It utilizes scalable servers, network components, and storage systems to provide the necessary resources for efficient email processing. This infrastructure is optimized for performance, ensuring that emails are processed quickly and reliably.

Intelligent Routing: Cisco Secure Email includes intelligent routing capabilities to optimize email delivery. It analyzes factors such as network conditions, sender reputation, and recipient availability to determine the most efficient path for email transmission. By intelligently routing emails, the solution reduces latency and ensures timely delivery.

Load Balancing: The solution supports load balancing mechanisms to distribute email processing across multiple servers or clusters. By balancing the workload, it ensures that no single component is overloaded, allowing for efficient utilization of resources and faster email processing.

Optimization for Latency Reduction: Cisco's solution incorporates various optimization techniques to minimize latency and improve email processing speed. This includes techniques like caching commonly accessed data, minimizing network round trips, and optimizing database queries. By reducing latency, the solution enables timely email delivery.

Real-Time Monitoring and Analytics: Cisco Secure Email offers real-time monitoring and analytics capabilities, providing insights into email processing performance. Administrators can track metrics such as email throughput, processing times, and delivery rates. This visibility allows for proactive monitoring and troubleshooting to address any performance bottlenecks promptly.

In summary, Cisco's Secure Email solution is designed to process emails quickly and efficiently to ensure timely delivery. Through advanced email processing techniques, a robust infrastructure, intelligent routing, load balancing, latency reduction optimizations, and real-time monitoring, the solution prioritizes fast and reliable email processing. It helps organizations maintain efficient email communication and deliver messages in a timely manner.

6.1.15. Compatibility

The Solution shall have the ability to seamlessly integrate with other email systems and protocols.

RESPONSE:

Cisco's Secure Email solution offers seamless integration with other email systems and protocols, ensuring compatibility and interoperability with various email environments. The solution is designed to integrate with different email architectures and can work alongside existing email infrastructure. Here's how Cisco Secure Email addresses this requirement:

Email Protocol Support: Cisco's solution supports standard email protocols such as SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol 3), and IMAP (Internet Message Access Protocol). This allows for seamless integration with different email systems and ensures compatibility with a wide range of email clients and servers.

Transparent Deployment: Cisco Secure Email can be deployed transparently within the existing email flow. It can function as a mail exchange gateway or relay, seamlessly integrating into the email infrastructure without disrupting the existing email systems or requiring major configuration changes.

Directory Integration: The solution supports directory integration, allowing for smooth integration with existing user directories such as Active Directory or LDAP (Lightweight Directory Access Protocol). This enables user synchronization and simplifies the management of email accounts and permissions across different systems.

Multi-vendor Support: Cisco's solution is designed to integrate with multi-vendor environments. It can seamlessly integrate with email systems from different vendors, providing flexibility and interoperability across diverse email environments. Whether your organization uses Microsoft Exchange, IBM Domino, Google Workspace, or other email systems, Cisco Secure Email can integrate and operate seamlessly.

API and Integration Framework: Cisco Secure Email offers APIs (Application Programming Interfaces) and integration frameworks that allow for custom integrations and extensions. This enables organizations to integrate the solution with other security tools, reporting systems, or custom workflows, providing a tailored and comprehensive email security ecosystem.

Hybrid Deployment Support: Cisco's solution supports hybrid email deployments, where organizations may have a combination of on-premises and cloud-based email systems. It can seamlessly integrate and secure email traffic across both environments, providing consistent protection and functionality.

In summary, Cisco's Secure Email solution offers seamless integration with other email systems and protocols. It supports standard email protocols, transparent deployment options, directory integration, multi-vendor environments, APIs and integration frameworks, and hybrid deployment support. These capabilities ensure smooth interoperability and compatibility with various email environments, allowing organizations to integrate the solution into their existing email infrastructure without disruptions.

6.1.16. Customization

The Solution shall offer a range of customization options to meet the specific needs of the organization and a user-friendly interface that is easy to set up and manage.

RESPONSE:

Cisco's Secure Email solution offers a range of customization options to meet the specific needs of organizations. The solution provides flexibility in configuration, policy settings, and user management to tailor the email security environment according to unique requirements.

Additionally, Cisco prioritizes a user-friendly interface that is easy to set up and manage. Here's how Cisco Secure Email addresses these requirements:

Configuration Flexibility: Cisco's solution allows for granular configuration and customization to align with the specific needs of the organization. Administrators can define and fine-tune security policies, spam thresholds, attachment handling, URL filtering rules, and other parameters to match the organization's security requirements and compliance policies.

Policy Settings: The solution provides comprehensive policy settings that enable organizations to enforce email security policies according to their specific needs. Administrators can define policies for spam detection, malware detection, data loss prevention (DLP), encryption, and more. These policies can be tailored to the organization's industry, regulatory requirements, and internal security standards.

User Management: Cisco Secure Email offers user management features to streamline user administration and access controls. The solution supports integration with existing user directories, simplifying user provisioning and authentication processes.

User-Friendly Interface: Cisco's solution prioritizes a user-friendly interface that is intuitive and easy to use. The management console provides a clear and organized layout, streamlined navigation, and contextual guidance to assist administrators in configuring and managing email security settings. The interface is designed to minimize complexity and ensure efficient setup and ongoing management of the solution.

Quick Setup and Deployment: Cisco Secure Email offers simplified and streamlined setup processes, allowing organizations to quickly deploy and activate the solution. The setup wizard guides administrators through the initial configuration steps, ensuring a smooth and efficient deployment experience. Additionally, the solution provides default security policies and recommendations to help organizations get started quickly while still allowing for customization as needed.

Documentation and Support: Cisco provides comprehensive documentation and support resources to assist organizations in setting up and managing Secure Email. This includes detailed guides, knowledge bases, FAQs, and access to technical support channels. These resources aim to provide organizations with the necessary guidance and assistance to effectively configure and manage the solution.

In summary, Cisco's Secure Email solution offers a range of customization options to meet the specific needs of organizations. It provides flexibility in configuration, policy settings, and user management. Additionally, the solution offers a user-friendly interface for easy setup and ongoing management. By combining customization options, user-friendly interfaces, and comprehensive support resources, Cisco Secure Email enables organizations to tailor their email security environment while simplifying administration and ensuring a smooth user experience.

6.1.17. Administration and Configuration

The Solution shall provide robust administrative capabilities that allow organizations to manage and customize their email security policies and settings. Some of the key administrative capabilities include:

6.1.17.1.

Policy Management: The Solution shall provide the ability to create and enforce email security policies that align with the Customer's security requirements. This shall include policies for anti-spam, anti-phishing, anti-malware, data loss prevention, and encryption.

RESPONSE:

Cisco's Secure Email solution provides extensive policy management capabilities, allowing organizations to create and enforce email security policies that align with their specific security requirements. The solution encompasses various policies to address anti-spam, anti-phishing, anti-malware, data loss prevention (DLP), and encryption. Here's how Cisco Secure Email addresses this requirement:

Anti-Spam Policy: Cisco's solution enables the creation and enforcement of anti-spam policies. Administrators can define thresholds and actions to be taken for identifying and handling spam emails. This includes options for marking, quarantining, or blocking spam messages based on various criteria such as spam scores, content analysis, and sender reputation.

Anti-Phishing Policy: The solution allows organizations to establish anti-phishing policies to combat phishing attacks. Administrators can configure rules to identify and block suspicious emails that attempt to deceive users or impersonate trusted entities. This includes analyzing email headers, URLs, content, and sender information to detect phishing indicators and take appropriate actions.

Anti-Malware Policy: Cisco Secure Email supports anti-malware policies to detect and prevent the delivery of malicious attachments or embedded malware. Administrators can define rules to scan attachments and emails for known malware signatures, behavior-based indicators, or heuristics. Detected malware can be quarantined, blocked, or subjected to further analysis and remediation actions.

Data Loss Prevention (DLP) Policy: The solution offers comprehensive DLP capabilities, allowing organizations to create and enforce policies to prevent the unauthorized disclosure of sensitive information. Administrators can define rules based on content analysis, keyword matching, or pattern recognition to identify and block emails containing sensitive data. This includes options for customizing policy actions such as blocking, encrypting, or flagging messages that violate DLP policies.

Encryption Policy: Cisco Secure Email supports encryption policies to secure sensitive communications. Administrators can configure policies to automatically encrypt emails based on specific criteria such as sender, recipient, or content. The solution can integrate with encryption technologies or provide built-in encryption capabilities to protect sensitive information transmitted via email.

Cisco's Secure Email solution provides a user-friendly management interface, allowing administrators to easily configure, enforce, and manage these email security policies. Through the policy management features, organizations can align their email security practices with their specific security requirements, enhance protection against threats, and enforce compliance standards.

It's important to note that specific policy management options and capabilities may vary based on the configuration and customization of Cisco's Secure Email solution.

6.1.17.2.

User Management: The Solution shall provide the ability to manage user accounts, roles, and permissions. This shall include the ability to create and delete user accounts, manage access rights, and configure authentication mechanisms such as single sign-on (SSO).

RESPONSE:

Cisco's Secure Email solution offers comprehensive user management capabilities, allowing organizations to effectively manage user accounts, roles, permissions, and authentication mechanisms. The solution provides the necessary tools to create and delete user accounts, manage access rights, and configure authentication options, including single sign-on (SSO). Here's how Cisco Secure Email addresses this requirement:

User Account Management: The solution enables administrators to manage user accounts within the Secure Email environment. This includes creating new user accounts, modifying user details, and deleting user accounts as needed. User accounts can be associated with specific email addresses, roles, and permissions to ensure appropriate access control.

Role-Based Access Control: Cisco's solution supports role-based access control (RBAC), allowing administrators to define roles with specific sets of permissions. By assigning users to roles, administrators can control the actions and functionalities available to each user. This ensures that access rights are appropriately assigned based on job responsibilities and security requirements.

Access Rights Management: The solution offers granular access rights management, enabling administrators to define and manage access permissions for individual users or groups. Administrators can specify permissions for various actions, such as configuring security settings, managing policies, accessing reports, or performing specific administrative tasks. This allows for fine-grained control over user capabilities within the Secure Email environment.

Authentication Mechanisms: Cisco Secure Email supports various authentication mechanisms, including single sign-on (SSO) options. Administrators can configure SSO integration with identity providers (IdPs) such as Active Directory Federation Services (ADFS), Security Assertion Markup Language (SAML) providers, or other SSO providers. This simplifies user authentication and streamlines access management by leveraging existing authentication infrastructure.

User Directory Integration: The solution integrates with user directories, such as Active Directory or LDAP, to streamline user management and authentication. User accounts and attributes can be synchronized from the existing directory, simplifying the user provisioning and ensuring consistency with the organization's user management practices.

Self-Service Capabilities: Cisco's solution may offer self-service capabilities, allowing users to manage certain aspects of their accounts, such as password resets or profile updates. Self-service options empower users to maintain their account information and reduce the administrative burden on IT teams.

In summary, Cisco's Secure Email solution provides robust user management capabilities, including user account management, role-based access control, access rights management, authentication mechanisms (including SSO), user directory integration, and self-service capabilities. These features enable organizations to effectively manage user accounts, control access rights, and configure authentication options within the Secure Email environment, ensuring secure and streamlined user administration.

6.1.17.3.

Configuration Management: The Solution shall provide the ability to configure email security settings such as transport rules, content filtering, quarantine settings, and notification settings. This shall include the ability to customize the security settings based on the organization's specific requirements.

RESPONSE:

Cisco's Secure Email solution offers extensive configuration management capabilities, allowing organizations to customize email security settings to meet their specific requirements. The solution provides flexibility in configuring transport rules, content filtering, quarantine settings, and notification settings. Here's how Cisco Secure Email addresses this requirement:

Transport Rules: Cisco's solution enables administrators to define and manage transport rules to control email flow and enforce specific policies. Transport rules can be configured based on criteria such as sender, recipient, subject, attachment type, or content. Administrators can specify actions to be taken when a rule is matched, such as blocking, quarantining, redirecting, or applying encryption to emails.

Content Filtering: The solution provides robust content filtering capabilities to detect and handle emails based on their content. Administrators can customize content filters to analyze email body, subject lines, attachments, or embedded URLs for specific keywords, patterns, or predefined rules. Content filtering can be used to identify and take actions on sensitive information, inappropriate content, or compliance-related concerns.

Quarantine Settings: Cisco Secure Email allows administrators to configure quarantine settings to manage and review potentially suspicious or unwanted emails. Administrators can define criteria for quarantining emails based on factors like spam score, virus detection, attachment types, or DLP violations. Quarantined emails can be reviewed, released, or deleted based on organizational policies.

Notification Settings: The solution offers configurable notification settings to keep administrators informed about important events and security incidents. Administrators can define notification preferences and thresholds for events such as spam detection, virus outbreaks, policy violations, or quarantine activities. Notifications can be sent via email or integrated with existing alerting systems for efficient monitoring.

Customization Options: Cisco's solution provides customization options to tailor the email security settings to the organization's specific requirements. This includes fine-tuning spam thresholds, adjusting security policy actions, configuring allowed/blocked lists, customizing quarantine settings, and adapting other security parameters. These customization options ensure that the email security settings align with the organization's security policies and compliance needs.

Centralized Management: Cisco Secure Email offers centralized management capabilities, providing a single console for configuring and managing email security settings across the organization. Administrators can access a unified interface to efficiently manage transport rules, content filtering, quarantine settings, notification settings, and other configuration parameters. This simplifies the management process and ensures consistent security configurations.

In summary, Cisco's Secure Email solution offers extensive configuration management capabilities, allowing organizations to customize email security settings based on their specific requirements. With features such as transport rules, content filtering, quarantine settings, notification settings, and customization options, the solution empowers administrators to tailor the email security environment to align with organizational policies and achieve effective protection against threats.

6.1.17.4.

Reporting and Analytics: The Solution shall provide the ability to generate detailed reports on email traffic, security incidents, policy violations, and user activity. This shall include the ability to customize and schedule reports for compliance and auditing purposes.

RESPONSE:

Cisco's Secure Email solution offers robust reporting and analytics capabilities, allowing organizations to generate detailed reports on email traffic, security incidents, policy violations, and user activity. The solution provides customization options and scheduling features to meet compliance and auditing requirements. Here's how Cisco Secure Email addresses this requirement:

Email Traffic Reports: The solution provides comprehensive reports on email traffic, including metrics such as email volume, delivery status, sender/receiver information, and traffic patterns. These reports offer insights into overall email activity, helping administrators monitor email usage, identify trends, and analyze traffic patterns.

Security Incident Reports: Cisco Secure Email generates reports on security incidents, providing visibility into detected threats such as spam, malware, and phishing attacks. These reports include details on the types of threats, affected email accounts, and actions taken by the security solution. Administrators can review and analyze security incident reports to gain insights into the effectiveness of the email security measures in place.

Policy Violation Reports: The solution offers reports specifically focused on policy violations. These reports highlight instances where emails have violated defined security policies, DLP rules, encryption requirements, or other compliance guidelines. Administrators can review policy violation reports to identify areas of non-compliance, adjust policies if necessary, and take appropriate actions to address policy violations.

User Activity Reports: Cisco's solution provides user activity reports to monitor and analyze email-related actions by individual users. These reports offer insights into email usage patterns, email volume, email traffic, and interactions with policy controls. User activity reports can help administrators identify abnormal behavior, detect insider threats, and ensure compliance with acceptable use policies.

Customization and Scheduling: Cisco Secure Email allows customization of reports to meet specific requirements. Administrators can select report parameters, such as timeframes, data filters, and report layouts, to generate reports tailored to their needs. The solution also offers scheduling options to automate report generation and distribution, ensuring that reports are delivered at specified intervals for compliance, auditing, or management purposes.

Compliance and Auditing Support: The solution provides reporting features that support compliance and auditing requirements. Reports can be customized to address specific regulatory frameworks or internal policies. Administrators can generate reports on security incidents, policy violations, user activity, and other metrics to demonstrate compliance, facilitate audits, and provide evidence of adherence to security and privacy standards.

In summary, Cisco's Secure Email solution offers powerful reporting and analytics capabilities. With detailed reports on email traffic, security incidents, policy violations, and user activity, the solution empowers administrators to monitor, analyze, and assess the effectiveness of their email security measures. Customization options and scheduling features further enhance the solution's flexibility in meeting compliance and auditing needs.

6.1.17.5.

Integration and Automation: The Solution shall provide the ability to integrate with other security solutions and automate routine tasks such as policy updates, threat detection, and incident response. This shall include the ability to leverage APIs and connectors to integrate with third-party security solutions.

RESPONSE:

Cisco's Secure Email solution offers robust integration and automation capabilities, allowing organizations to integrate with other security solutions and automate routine tasks. The solution provides APIs, connectors, and automation features to facilitate seamless integration and streamline security operations. Here's how Cisco Secure Email addresses this requirement:

API Integration: Cisco's solution offers APIs (Application Programming Interfaces) that enable integration with other security solutions and third-party applications. These APIs allow for the exchange of information, facilitating coordinated threat detection, incident response, and policy enforcement across the security ecosystem. Integration via APIs allows organizations to leverage the strengths of multiple security solutions, creating a more comprehensive and cohesive security posture.

Connectors and Integrations: Cisco Secure Email provides pre-built connectors and integrations with other security solutions, such as SIEM (Security Information and Event Management) systems or threat intelligence platforms. These connectors enable seamless data sharing, allowing organizations to centralize and correlate security events, threat intelligence, and email security data for enhanced visibility and streamlined incident response.

Automation Framework: The solution incorporates automation capabilities to streamline routine tasks and security operations. Administrators can define workflows and automation rules to automate policy updates, threat detection, incident response actions, and other repetitive tasks. This reduces manual effort, improves efficiency, and ensures consistent application of security measures.

Orchestration and Response: Cisco Secure Email integrates with security orchestration, automation, and response (SOAR) platforms. This enables organizations to orchestrate email security actions and responses with other security tools, incident response processes, and playbooks. By leveraging SOAR capabilities, organizations can automate incident handling, enforce coordinated responses, and optimize security operations.

Event and Log Management: The solution provides event and log management features, allowing organizations to collect, analyze, and correlate security events and logs from various sources. This includes events generated by the Secure Email solution itself as well as logs from integrated systems. Centralized event and log management facilitate comprehensive threat analysis, incident investigation, and compliance reporting.

Threat Intelligence Integration: Cisco's solution integrates with threat intelligence feeds and platforms to leverage external threat intelligence data. This enables the solution to enrich its email security capabilities with up-to-date threat information, improving detection and response to emerging threats. By integrating threat intelligence, organizations can benefit from a more comprehensive and proactive defense against email-based threats.

In summary, Cisco's Secure Email solution offers robust integration and automation capabilities. Through APIs, connectors, automation frameworks, and integrations with other security solutions, the solution enables organizations to integrate their email security with the broader security ecosystem. This allows for coordinated threat detection, incident response, and policy enforcement. By leveraging integration and automation, organizations can enhance their overall security posture and security operations.

6.1.17.6.

Audit and Compliance: The Solution shall provide the ability to track and log all email-related activities and events to ensure compliance with regulatory and industry standards. This shall include the ability to generate audit trails, provide access logs, and support eDiscovery requests.

RESPONSE:

Cisco's Secure Email solution provides robust audit and compliance capabilities to track and log email-related activities and events. The solution ensures compliance with regulatory and industry standards by generating audit trails, providing access logs, and supporting eDiscovery requests. Here's how Cisco Secure Email addresses this requirement:

Audit Trail Generation: The solution generates comprehensive audit trails that capture email-related activities and events. This includes information such as email delivery, policy enforcement, threat detection, user actions, and system events. Audit trails provide a detailed record of email activities, allowing organizations to track and review events for compliance, forensic investigations, or internal auditing purposes.

Access Logs: Cisco's solution maintains access logs that record user access and actions within the Secure Email environment. Access logs provide visibility into administrative activities, configuration changes, and policy updates. These logs help organizations track user actions, enforce accountability, and monitor compliance with security policies.

Compliance Reporting: Cisco Secure Email offers reporting features that support compliance requirements. Organizations can generate reports that demonstrate adherence to regulatory frameworks such as GDPR, HIPAA, or industry-specific standards. Compliance reports provide an overview of email security measures, policy enforcement, threat detection, and other relevant metrics to meet audit and compliance needs.

eDiscovery Support: The solution supports eDiscovery requests by providing the necessary tools and capabilities to search, retrieve, and export email-related data for legal or investigative purposes. Administrators can conduct searches based on specified criteria such as sender, recipient, subject, date range, or keywords. The solution facilitates efficient retrieval and export of relevant email data to meet eDiscovery requirements.

Data Retention: Cisco Secure Email offers data retention capabilities, allowing organizations to retain email data for compliance and legal purposes. Administrators can define retention policies to specify how long email data should be retained. This helps organizations meet regulatory requirements for data retention and ensures the availability of historical email data for auditing or eDiscovery needs.

In summary, Cisco's Secure Email solution provides robust audit and compliance capabilities. By generating audit trails, maintaining access logs, supporting compliance reporting, facilitating eDiscovery requests, enabling data retention, and offering legal hold functionality, the solution assists organizations in meeting regulatory requirements, enforcing accountability, and addressing legal and investigative needs.

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's Secure Email solution is designed to comply with relevant standards and regulations, including those mentioned such as General Data Protection Regulation (GDPR), Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), 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. Cisco recognizes the importance of meeting these compliance requirements and offers features and capabilities to support organizations in achieving and maintaining compliance. Here's how Cisco Secure Email addresses these compliance requirements:

GDPR Compliance: Cisco's solution provides features to help organizations meet GDPR requirements. It includes capabilities for data protection, consent management, data retention policies, and the ability to respond to data subject access requests. These features support organizations in aligning with GDPR principles for the protection and privacy of personal data.

CJIS Compliance: Cisco Secure Email has the flexibility to meet CJIS compliance requirements. The solution supports encryption, access controls, audit trails, and other security measures to protect Criminal Justice Information Services data. Cisco is committed to working with organizations and signing the necessary CJIS riders or security agreements to support compliance with CJIS requirements.

HIPAA Compliance: Cisco's solution supports HIPAA compliance requirements for safeguarding protected health information (PHI). It includes features such as encryption, access controls, auditing capabilities, and security incident response to help organizations meet HIPAA's security and privacy requirements.

FERPA Compliance: Cisco Secure Email can assist organizations in complying with FERPA, which protects the privacy of student education records. The solution provides security controls and features to safeguard sensitive student information, ensuring compliance with FERPA regulations.

PII Data Requirements: Cisco's solution addresses the protection of personally identifiable information (PII) through a combination of security measures. This includes encryption, access controls, data loss prevention (DLP), and other features to safeguard PII data from unauthorized access, disclosure, or misuse.

Driver Privacy Protection Act Compliance: Cisco Secure Email can assist organizations in meeting the requirements of the Driver Privacy Protection Act (DPPA), which regulates the use and disclosure of personal information obtained from motor vehicle records. The solution provides security controls and features to protect the privacy of driver-related information.

Third-Party Certifications: Cisco has obtained various third-party certifications, including Systems and Organizations Controls 2 (SOC 2) and International Organization for Standardization (ISO) 27001. These certifications validate the implementation of robust security controls, processes, and compliance practices within Cisco's operations and solutions.

Cisco understands that security agreements, such as CJIS riders or Business Associate Agreements, may be required by the Department, Purchaser, or Customer. Cisco is committed to working with organizations to address these requirements and is willing to execute necessary security agreements as a condition of performance or purchase order issuance.

In summary, Cisco's Secure Email solution is designed to comply with relevant standards and regulations, including GDPR, CJIS, HIPAA, FERPA, PII data requirements, DPPA, SOC 2, and ISO 27001. By incorporating appropriate security controls, features, and certifications, Cisco Secure Email helps organizations meet compliance requirements and supports the execution of necessary security agreements as required.

6.1.19. Integration

6.1.19.1.

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:

Cisco's Secure Email solution is designed to integrate seamlessly with existing security tools, including firewalls, antivirus software, endpoint management solutions, and security information and event management (SIEM) systems. The solution offers integration capabilities that allow for a coordinated and consolidated security ecosystem. Here's how Cisco Secure Email addresses this requirement:

Firewall Integration: Cisco's solution can integrate with the Department's existing firewalls to enhance overall network security. Integration with firewalls allows for coordinated threat prevention and enables the enforcement of consistent security policies across different security layers.

Antivirus Software Integration: Cisco Secure Email can integrate with antivirus software to provide comprehensive protection against email-borne malware. By integrating with existing antivirus solutions, the solution leverages multiple layers of defense to detect and block malicious attachments or embedded malware in emails.

Endpoint Management Solutions Integration: The solution can integrate with endpoint management solutions to extend email security measures to endpoints, ensuring consistent protection across the entire network. Integration allows for coordinated threat detection and response, including the identification of email-related security incidents on endpoints.

SIEM Integration: Cisco's solution supports integration with SIEM systems for centralized event correlation, analysis, and monitoring. By integrating with SIEM, security events, and logs from Cisco Secure Email can be aggregated with data from other security solutions. This facilitates comprehensive threat detection, incident response, and compliance reporting across the security ecosystem.

Custom Integration Support: Cisco recognizes that each Customer's security environment may vary. The solution provides the necessary tools, APIs, and documentation to support custom integrations with specific security tools or systems. This allows Customers to determine the feasibility and requirements of integrating the solution with their existing security tools. The Contractor, Cisco, is committed to working with the Customer to ensure successful integration and taking any necessary steps to support Customer integration efforts.

In summary, Cisco's Secure Email solution offers integration capabilities with existing security tools such as firewalls, antivirus software, endpoint management solutions, and SIEM systems. Integration enhances overall security effectiveness by providing coordinated threat prevention, unified event monitoring, and consolidated incident response. The solution also supports custom integration to accommodate specific Customer requirements. Cisco is dedicated to assisting with integration efforts and ensuring a seamless integration experience.

6.1.19.2.

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

RESPONSE:

Cisco's Secure Email solution supports data integration through common exchange techniques and frameworks, including RESTful Application Programming Interfaces (APIs). The solution provides APIs that enable seamless data exchange and integration with other systems, applications, or frameworks. Here's how Cisco Secure Email addresses this requirement:

RESTful APIs: Cisco's solution offers RESTful APIs that provide a standardized and flexible approach for data integration. These APIs enable organizations to programmatically interact with Secure Email and exchange data with other systems or applications. Through RESTful APIs, organizations can retrieve email security data, configure settings, and perform various operations to integrate Secure Email into their existing workflows and processes.

Data Exchange: The RESTful APIs provided by Cisco Secure Email facilitate the exchange of data between the solution and external systems. Organizations can retrieve information such as email metadata, security events, policy violations, and threat intelligence data. This data can be integrated into other systems or frameworks for further analysis, reporting, or integration with broader security operations.

Event Notification: Cisco's solution supports event notifications via APIs, allowing organizations to receive real-time alerts and notifications about security events, policy violations, or other email-related activities. These notifications can be integrated with external systems or applications, enabling organizations to trigger automated responses, update dashboards, or initiate incident response workflows.

Integration with Security Operations: The RESTful APIs provided by Cisco Secure Email enable integration with security operations frameworks or security orchestration, automation, and response (SOAR) platforms. This allows organizations to streamline incident response workflows, automate security actions, and enhance coordination across security tools and systems.

Custom Integration: The solution provides the flexibility for custom integration using RESTful APIs. Organizations can leverage these APIs to build custom integrations with specific systems, applications, or frameworks that are critical to their security infrastructure. This allows for tailored integration to meet unique requirements and leverage the full capabilities of Cisco Secure Email.

In summary, Cisco's Secure Email solution supports data integration through common exchange techniques and frameworks such as RESTful APIs. By providing RESTful APIs, the solution enables seamless data exchange, event notification, and integration with external systems, applications, and security operations frameworks. Organizations can leverage these APIs to integrate Secure Email into their existing workflows, exchange data with other systems, and customize integrations to meet specific requirements.

6.1.19.3.

The Solution shall be capable of integrating with a variety of identity and access management (IAM) systems, as well as with the applications and systems that require authentication, to meet Customer current and future needs.

RESPONSE:

Cisco's Secure Email solution offers integration capabilities with a variety of identity and access management (IAM) systems, as well as with applications and systems that require authentication. The solution provides flexible integration options to meet Customer's current and future needs. Here's how Cisco Secure Email addresses this requirement:

Identity and Access Management (IAM) Integration: Cisco's solution supports integration with popular IAM systems, such as Active Directory, LDAP, or cloud-based IAM platforms. This allows organizations to leverage their existing IAM infrastructure for user provisioning, authentication, and access management in the Secure Email environment. Integration with IAM systems ensures consistent user identities, access controls, and policy enforcement across the organization.

Single Sign-On (SSO) Integration: Cisco Secure Email supports integration with SSO solutions, including SAML-based identity providers (IdPs) and other industry-standard SSO protocols. This enables seamless authentication and access to the solution using existing corporate credentials. SSO integration simplifies user authentication processes, enhances security, and improves user experience by eliminating the need for separate login credentials.

Multi-Factor Authentication (MFA) Integration: The solution can integrate with MFA solutions to provide an additional layer of security during authentication. Organizations can enforce MFA for accessing the Secure Email environment, adding an extra level of protection to prevent unauthorized access and enhance security posture.

Application and System Authentication: Cisco Secure Email integrates with applications and systems that require authentication, such as email clients, collaboration platforms, or custom applications. This ensures that users accessing these applications and systems are authenticated and authorized based on the organization's security policies and IAM configurations.

Future-Ready Integration: Cisco recognizes that customer needs evolve over time. The solution is designed with flexibility and extensibility to adapt to future IAM systems, authentication methods, or emerging standards. This ensures that Cisco Secure Email can accommodate changing customer requirements and integrate with new IAM technologies as they emerge.

In summary, Cisco's Secure Email solution provides integration capabilities with a variety of IAM systems, SSO solutions, MFA solutions, and applications/systems that require authentication. By integrating with IAM systems and authentication frameworks, the solution ensures consistent user management, access controls, and authentication processes. Cisco's solution also offers flexibility to support future IAM needs and evolving authentication technologies, providing organizations with a future-ready integration capability.

6.1.19.4.

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's Secure Email solution supports initial integration with the state Cybersecurity Operations Center (CSOC) and validates the proper integration of Solution data as requested by the Customer. Here's how Cisco Secure Email addresses this requirement:

CSOC Integration: Cisco's solution provides the necessary integration capabilities to connect with the state Cybersecurity Operations Center (CSOC). This integration allows for the exchange of security event information, threat intelligence data, and other relevant data between Cisco Secure Email and the CSOC. It enables organizations to benefit from the expertise and resources of the CSOC in monitoring, detecting, and responding to email-based threats.

Solution Data Validation: Cisco Secure Email ensures that all Solution data is properly integrated and validated as requested by the Customer. This includes verifying the correct flow of email-related security events, logs, and data to the CSOC for analysis and monitoring. Validation ensures that the data exchange is functioning as expected and provides assurance that the CSOC has access to relevant information for effective incident response and threat mitigation.

FL[DS] Compliance: Cisco's solution adheres to the requirements set forth by the FL[DS] (Florida Digital Service). The integration process considers the specific FL[DS] compliance guidelines, data handling protocols, and security standards to ensure that Solution data is securely transmitted and shared with the CSOC. Compliance with FL[DS] guidelines helps maintain data privacy, integrity, and confidentiality throughout the integration process.

Cisco is committed to working closely with the Customer to understand their specific integration requirements with the CSOC and FL[DS]. By leveraging the integration capabilities of Cisco Secure Email, organizations can establish a secure and efficient flow of Solution data to the CSOC for enhanced cybersecurity operations and collaborative threat defense.

Please note that the specifics of the integration process may vary depending on the Customer's requirements, CSOC's infrastructure, and FL[DS] guidelines. The integration process will involve coordination and collaboration between Cisco, the Customer, and relevant stakeholders to ensure a successful and compliant integration.

Cisco can provide a cost estimate once requirements are more clearly defined.

6.1.19.5.

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.

RSEPONSE:

Cisco understands that integration maintenance may be required after the initial integration to ensure the proper exchange of data between Customers and the state Cybersecurity Operations Center (CSOC). The Contractor, Cisco, is committed to addressing any concerns raised by the FL[DS] regarding integration issues. Here's how Cisco Secure Email addresses this requirement:

Ongoing Integration Support: Cisco provides ongoing support to address integration issues and maintain the smooth flow of data between Customers and the CSOC. This includes troubleshooting any technical issues, resolving connectivity problems, and ensuring the continuous exchange of relevant security event information, threat intelligence data, and other required data.

Proactive Monitoring and Maintenance: Cisco actively monitors the integration between the Solution and the CSOC to identify any potential issues or anomalies. Through proactive monitoring and regular maintenance, Cisco aims to ensure the integrity and reliability of the integration, addressing any concerns promptly.

Collaboration with FL[DS]: Cisco collaborates closely with the FL[DS] to address any concerns they may have regarding integration issues. The Contractor actively engages in communication, coordination, and collaboration with FL[DS] stakeholders to understand their requirements, resolve any integration-related concerns, and ensure compliance with FL[DS] guidelines.

Timely Issue Resolution: Cisco is committed to providing timely resolution of any integration issues that may arise. The Contractor acknowledges the importance of maintaining the proper exchange of data between Customers and the CSOC and promptly addresses any concerns or challenges that may impact the integration process.

Continuous Improvement: Cisco strives for continuous improvement in the integration process to enhance the efficiency, reliability, and security of data exchange between Customers and the CSOC. The Contractor actively incorporates feedback from the FL[DS] and other stakeholders to optimize integration practices and ensure a seamless flow of data.

By offering ongoing integration support, proactive monitoring and maintenance, collaboration with the FL[DS], timely issue resolution, and a commitment to continuous improvement, Cisco addresses concerns and ensures the proper functioning of the integration between the Solution and the CSOC. This helps maintain a robust and effective cybersecurity defense ecosystem for Customers.

Please note that the specific integration maintenance process may vary based on the Customer's requirements, CSOC's infrastructure, and FL[DS] guidelines. The Contractor will work closely with the Customer, FL[DS], and other relevant stakeholders to address any integration concerns and maintain a successful and compliant integration.

Cisco can provide a cost estimate once requirements are more clearly defined.

6.1.20. 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.

6.1.20.1.

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

RESPONSE:

Cisco's Secure Email solution provides performance and availability Service Level Agreements (SLAs) to ensure the successful operation and availability of the Solution. While specific SLA terms may vary based on the contractual agreement, Cisco typically aims to deliver high-performance and availability objectives. Here's how Cisco Secure Email addresses performance and availability:

High Availability Architecture: Cisco's solution is designed with a highly available architecture to minimize downtime and ensure continuous service availability. Redundancy measures, fault tolerance, and failover mechanisms are implemented to provide resiliency and minimize disruptions.

Reliable Infrastructure: The underlying infrastructure supporting Cisco Secure Email is built to provide high reliability and availability. This includes data centers with redundant power, network connectivity, and storage systems, as well as comprehensive disaster recovery strategies.

Performance Optimization: Cisco continuously optimizes the performance of Secure Email to deliver fast and efficient email security services. Performance enhancements are implemented through various techniques such as load balancing, caching, and intelligent traffic management to ensure responsive and reliable email security operations.

Network Connectivity: Cisco maintains robust network connectivity to ensure optimal performance and availability of the Secure Email solution. Multiple network providers, diverse routing paths, and advanced network monitoring and management practices are employed to deliver reliable connectivity and minimize disruptions.

SLA Commitments: Cisco typically provides SLAs that outline performance and availability objectives for the Secure Email solution. While the specific SLA terms may vary based on the contractual agreement, Cisco strives to meet or exceed industry-standard objectives. A common

SLA target for availability is 99.999% uptime per month, indicating a commitment to ensuring the Solution is available for the vast majority of the time.

It's important to note that specific SLA terms and details, including performance metrics, uptime guarantees, and any associated remedies, are typically determined through contractual agreements between Cisco and the Customer. These SLAs are designed to provide transparency, accountability, and assurance regarding the performance and availability of the Secure Email solution.

When engaging with Cisco for Secure Email, Customers can discuss their specific performance and availability requirements, and Cisco can provide the appropriate SLA terms and commitments to align with their needs.

Please consult with Cisco or a qualified representative to obtain detailed SLA information that specifically addresses the performance and availability objectives you require for the Secure Email solution.

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 Email 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:

All subscriptions include Cisco Technical Assistance Center (TAC) support (24/7) and customer success for onboarding assistance. See Support document in Addendum I.

Cisco offers free on-demand online training.

c) Implementation Plan

RFQ Text:

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

Response:

Presidio has 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) Disaster Recovery Plan

RFQ Text:

A draft disaster recovery plan per section 30.5.

Response:

Cisco Secure Email aligns with the FLDS DR plan. Cisco's solution is hosted in 11 data centers, with 99.999% uptime.

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

Elche City Council Improves Email Security to Protect Local Citizens and Businesses

Elche City Council is the governing and administrative body of the municipality of Elche, Spain, with more than 2,000 employees and more than 140 administrative offices. The council is immersed in a digitization process that has, of necessity, been accelerated exponentially because of the pandemic. This process has produced a change in how the city approaches technology and hybrid work, and has helped demonstrate the value of digital transformation. As the digitization and cybersecurity projects have progressed, citizens, officials, and companies have realized the value of achieving IT security and resilience.

Customer Name: Elche City Council

Industry: Government

Number of Employees: 2000+

Challenges:

- Protect and encrypt communications with citizens and businesses
- Integration with Microsoft 365 email platform

Solutions:

- Cisco Secure Email

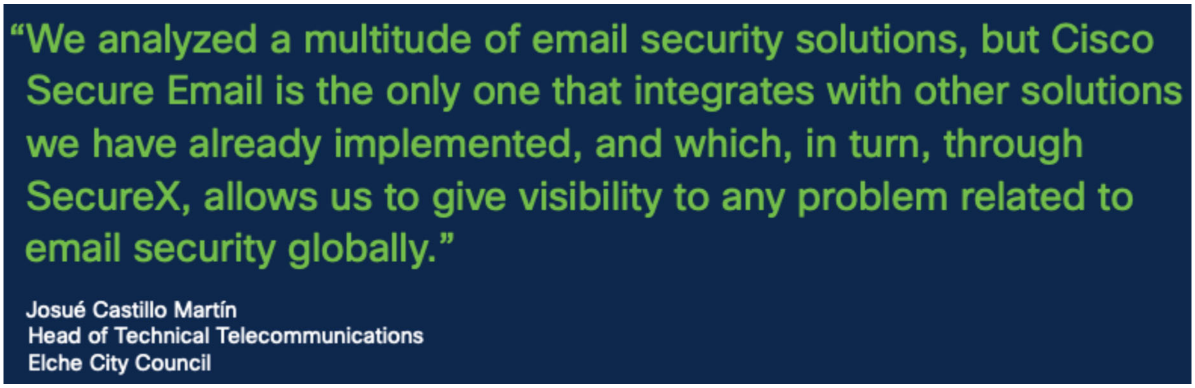
Results:

- Greater visibility into infrastructure
- Thousands of pieces of spam blocked daily
- Reduction in questions to technical support

The Elche City Council worked with Cisco Secure to implement Cisco Secure Email. The city chose the solution because of its ease of implementation, its integration with Microsoft 365, and the performance of Cisco Web Security.

The results were immediate. The city now has greater visibility into their infrastructure, and prevents thousands of spam from being delivered daily. With Cisco Secure Email, the city has seen a reduction in questions coming into their technical department, which frees those workers for other city initiatives and priorities.

The Elche City Council values the partnership they have with Cisco Secure, city leaders say, and the quality of service, speed of technical support, and sharing of best practices have made Cisco Secure Email a valuable security solution for the city.



> "We analyzed a multitude of email security solutions, but Cisco Secure Email is the only one that integrates with other solutions we have already implemented, and which, in turn, through SecureX, allows us to give visibility to any problem related to email security globally."
>
> **Josué Castillo Martín**
> **Head of Technical Telecommunications**
> **Elche City Council**

3) IMPLEMENTATION

RFQ Text:

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

Response:

Included in the Price Sheet is an initial implementation based on a fixed scope of rules, details below. Price per Entity: $20,000

Scope includes:

Cisco Secure Email Cloud Gateway

- Initial cloud portal configuration
- AD integration for account and group mappings
- Creating the user accounts for quarantine
- Review policies for relevance and accuracy before being migrated to Secure Email Cloud Gateway
- Review and configure basic email routing (Mail Routing)
  - Configure up to 4 Email Inbound Rules
- Configure Domains for which you receive mail
  - Configure up to five (5) domains, hosts, or subnets
- Configure up to fifty (50) custom rules/filters
- Review and configure security and SPAM services
- Cutover of the MX record to the solution so that it becomes the front end of all inbound and outbound email traffic

Note: DLP, Secure Email Encryption Service, and Graymail Safe Unsubscribe is NOT included as part of this scope of work

1.1.1. Client Responsibilities:

- Client is responsible for configuration (including removal) of any existing email security product integrations
- Client is responsible for configuration of their email platform(s) including, but not limited to, O365/Exchange
- Client will prepare a test plan to execute before and after tests and cutover

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.

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

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

  - 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.

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. The vendor shall provide pricing for Section III below for Secure Email Gateway (SEG) and/or Section IV below for Integrated Cloud Email Security (ICES). FL[DS] anticipates purchasing the email security 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 - Secure Email Gateway (SEG)

Initial Term Pricing (Years 1-3)		
Item No.	**Description**	**Annual Rate Per User**
1	**Initial Software Year** One year of SEG software Solution as described in the RFQ per user. To include: • **implementation** • **initial training** • **initial Integration** • integration maintenance	$ 43.70 per user for up to 100 users* $20,000 Implementation Services per entity *Waterfall pricing available for larger user count.

	• support services	
2	**Subsequent Software Year** One year of SEG software Solution as described in the RFQ per user. To include: • **ongoing training** • integration maintenance • support services	$ 50.25 per user for up to 100 users* *Waterfall pricing available for larger user count.
Optional Renewal Term Pricing (Years 4-6)		
Item No.	**Description**	**Rate Per User**
1	**Initial Software Year** One year of SEG software Solution as described in the RFQ per user. To include: • **implementation** • **initial training** • **initial Integration** • integration maintenance • support services	$ 66.46 per user for up to 100 users* *Waterfall pricing available for larger user count.
2	**Subsequent Software Year** One year of SEG software Solution as described in the RFQ per user. To include: • **ongoing training** • integration maintenance • support services	$ 76.43 per user for up to 100 users* *Waterfall pricing available for larger user count.

LICENSE TRANSFERABILITY: The licenses may transfer between Customer (Entity) and Purchaser based upon funding for each fiscal year.

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

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 rate shown.

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**
CSEMAIL-SEC-SUB	Cisco Secure Email XaaS Subscription	$0	$0	$0
SVS-EMAILC-SUP-E	Enhanced Support for Cisco Email Security	$1	$.90	$0.38
SVS-EMAILC-SUP-P	Premium Support for Cisco Email Security	$1	$.90	$0.38
CES-ADV-LIC	Cisco Secure Email Cloud Advantage, Essential+ GSU+DLP+ENC	$55.62	$50.06	$20.18
CES-IMD-LIC	Cisco Internal Mailbox Defense License	$16.15	$15.34	$7.92
CES-MA-ULTD-LIC	Cisco Secure Email Cloud Malware Analytics Unlimited License	$0	$0	$0
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**

CSEMAIL-SEC-SUB	Cisco Secure Email XaaS Subscription	$0	$0	$0
SVS-EMAILC-SUP-E	Enhanced Support for Cisco Email Security	$1	$.90	$0.38
SVS-EMAILC-SUP-P	Premium Support for Cisco Email Security	$1	$.90	$0.38
CES-ADV-LIC	Cisco Secure Email Cloud Advantage, Essential+ GSU+DLP+ENC	$55.62	$50.06	$20.18
CES-IMD-LIC	Cisco Internal Mailbox Defense License	$16.15	$15.34	$7.92
CES-MA-ULTD-LIC	Cisco Secure Email Cloud Malware Analytics Unlimited License	$0	$0	$0

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.

User Quantity	Annual Rate Per User	Implementation Services per Entity	Annual Rate per Entity
100	$43.70	$20,000	$24,369.96
500	$38.39	$20,000	$39,197.16
1000	$33.53	$20,000	$53,532.71
5000	$25.10	$20,000	$145,518.24
10000	$23.64	$20,000	$256,412.58
25000	$13.70	$20,000	$362,472.31

Renewals after FY 23-24 will have a ceiling rate of 15% increase year over year. Actual renewal rate may be lower than ceiling rate.

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.

Presidio Networked Solutions, LLC
Vendor Name

Erik Hayko
Signature

58-1667655
FEIN

Erik Hayko
Signatory Printed Name

May 24, 2023
Date

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

8) ADDENDUM I

Cisco’s Support documentation in the pages below.

Cisco Severity and Escalation Guidelines

When you are submitting a problem to Cisco, assign a Severity Level as follows:

Table 1. Severity Levels

Severity Level	Description
Severity 1	An existing Network or Environment is down or there is a critical impact to End User's business operation. End User and Cisco both will commit full-time resources to resolve the situation.
Severity 2	Operation of an existing Network or Environment is severely degraded or significant aspects of End User's business operation are negatively impacted by unacceptable Network or Environment performance. End User and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.
Severity 3	Operational performance of the Network or Environment is impaired, although most business operations remain functional. End User and Cisco both are willing to commit resources during Standard Business Hours to restore service to satisfactory levels.
Severity 4	Information is required on Cisco product capabilities, installation, or configuration. There is little or no impact to End User's business operation. End User and Cisco both are willing to provide resources during Standard Business Hours to provide information or assistance as requested.

Notifications of Severity 1 and Severity 2 cases that are in a Cisco pending state are automatically sent to leadership based on the following schedule.

Table 2. Automatic Escalation Process

Elapsed Time	Severity 1	Severity 2	Severity 3	Severity 4
1 hour	TAC Team Lead			
2 Hour	TAC Manager			
4 hours	TAC Director	TAC Team Lead		
5 Hours		TAC Manager		
12 Hours	TAC Director Second Alert			
24 hours	TAC Vice President/Sr. Vice President	TAC Sr. Manager/Director		
48 hours	CEO	TAC Vice President/Sr. Vice President		
72 hours				
96 hours		CEO		

Severity 1 and 2 escalation times are measured in calendar hours—24 hours per day, 7 days per week.

If you do not believe that adequate progress is being made regarding resolution of a properly submitted problem, you may escalate the problem to the on-shift duty manager.

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 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.

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

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 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) 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:

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.

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

Department of MANAGEMENT SERVICES
We Serve Those Who Serve Florida

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-22/23-161, Email Security 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: Pedro Allende
5E91A9D369EB47C...

Name: Pedro Allende

Title: Secretary

Date: 6/14/2023 | 5:00 PM EDT

Presidio Networked Solutions, LLC

By: ______________________

Name: Jay Staples

Title: Assistant General Counsel

Date: 5/24/2023