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-22/23-161A
BETWEEN
STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES
AND
OPTIV SECURITY INC.

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 OPTIV SECURITY INC. (Contractor), with offices at 2653 Scott Mill Lane, Jacksonville, FL 32223, 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:

Ed Topoleski
Client Manager
500 N. Westshore Blvd., Suite 950
Tampa, FL 33609
Telephone: (321) 277-1398
Email: Edward.topoleski@optiv.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 the necessary Department, Purchaser, and Customer personnel, as required, to answer questions and resolve issues. The Contractor must provide written notice to the Department's Contract Manager if a new employee is designated as the Contractor's Representative for this Contract.

9.0 Assignment

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

10.0 Price Decreases

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

11.0 Additions/Deletions

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

12.0 Cooperative Purchasing

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

13.0 Other Conditions

13.1 Independent Contractor Status

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

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

13.2 Force Majeure

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

13.3 Cooperation with the Florida Senate and Florida House of Representatives

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

13.4 Employment of State Workers

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

SIGNATURE PAGE IMMEDIATELY FOLLOWS

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

OPTIV SECURITY INC:	STATE OF FLORIDA DEPARTMENT OF MANAGEMENT SERVICES:
DocuSigned by: Liz Abram-Oldham 8CDCE9D09B524D9...	DocuSigned by: Pedro Allende 5E91A9D369EB47C...
Authorized Signature	Pedro Allende, Secretary
Liz Abram-Oldham	6/30/2023 | 10:47 PM EDT
Print Name	Date
Director of Contracts	
Title	
6/30/2023 | 8:24 PM MDT	
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:**

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

   OTHER PURCHASER:
   CONTRACT MANAGER SPECIFIED ON THE PO

20.3 Public Records Exemption

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

20.4 Document Management

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

21.0 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 Screening Compliance Audits and Security Inspections

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

32.7 Record Retention

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

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:		

Optiv Response for The State of Florida Department of Management Services (DMS)

Request for Quotes (RFQ) DMS-22/23-161

Email Security Solution

May 24th, 2023

Table of Contents

OPTIV

Denver Office
1144 15th Street, Suite 2900
Denver, CO 80202
800.574.0896
www.optiv.com

May 24th, 2023

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

Subject: Optiv Proposed Abnormal Solution for DMS-2223-161-Email Security Solution RFQ

Dear Alisha,

Thank you for the opportunity to provide you with a proposal to sell Abnormal Security to entities in the State of Florida.

Based on our vast experience in reselling Abnormal Security, we are confident we can assist you in achieving your objectives. Please feel free to reach out to me should you any questions and we look forward to working with you on this important engagement.

Sincerely,

Ed Topoleski

Client Manager

Optiv Security Inc.

Abnormal Overview

Abnormal

Abnormal for State and Local Government

Discover the AI-based email security platform that protects state and local governments from the full spectrum of email attacks.

10x	More Effective Solution for Email Security	3x	Fewer Attacks Get Through	2x	Faster Threat Response Time

Abnormal Overview

- Cloud-native email security platform that protects against the full spectrum of attacks and unwanted mail.
- API-based solution integrates with Microsoft 365 and Google Workspace in minutes.
- Behavioral AI baselines normal behavior to block deviations from known good.

What Sets Abnormal Apart

- No disruption to mail flow and no changes to MX records required.
- Protection against internal and external account compromise.
- AI-driven triage, investigation, and auto-remediation for more efficient SOC workflows.

Abnormal Integrates Quickly With:

- Secure email gateways and existing security layers for advanced protection.
- SIEM, SOAR, and other SOC solutions for fully automated workflows.
- Email security solution dashboards for single-source visibility into email threats, investigations, and trends.

Attackers Target Government Agencies for Valuable Data

Threat actors know that state and local governments have troves of data and access to critical operational processes. Unfortunately, they're also aware that these organizations often don't have enterprise-level security tools to keep them out. The result is an ongoing wave of disruptive, costly incidents involving city, county, and state agencies.

Legacy Security Tools Can't Block Advanced Threats

Traditional email security tools like secure email gateways aren't designed to detect advanced socially-engineered attacks. Modern threat actors exploit common psychological vulnerabilities as well as trusted names and relationships to trick or pressure recipients into sharing information, downloading malware, or transferring funds.

Modern Email Security for State and Local Governments

Abnormal's cloud-native solution integrates with Microsoft 365 and Google Workspace in minutes and uses thousands of signals across identity, behavior, and content to separate legitimate messages from dangerous threats. Because Abnormal recognizes anomalies even in ongoing conversations, it immediately detects and remediates threats that legacy systems miss—keeping governments secure and operational.

Email-Based Attacks Lead to Costly Incidents for State and Local Governments

$2.07M	2,792	$2.4B
Average cost of a public sector data breach.	Number of successful data compromise attacks targeting government agencies in 2022.	Total business email compromise losses reported to the FBI in 2021.

Source: 2022 IBM Cost of a Data Breach Report

Source: 2022 Verizon Data Breach Investigations Report

Source: 2021 FBI IC3 Report

Abnormal for State and Local Government

Stop the most dangerous attacks that bypass your existing defenses.

Ransomware

In 2021, local government entities were the second-highest targeted group for ransomware attacks. These attacks can disrupt educational facilities, emergency services, critical utilities, and other government-run services.

How Abnormal Stops Ransomware:

Analyzes message content and other signals for credential phishing

Utilizes identity detection and natural language processing (NLP) to spot first-stage attacks like phishing, even those coming from trusted senders.

Blocks malicious attachments and links

Reviews all attachments and links for safety, including links that redirect upon clicking.

Gives security teams explainable insights and malware forensics

Automatically prepares detailed analyses of ransomware attempts, enabling teams to preview attachment content and link targets.

Supply Chain Compromise

Because state and local government agencies often share details of their current and past contracts on their websites, it's easy for attackers to gather the information they need to impersonate vendors via email to commit invoice and payment fraud.

How Abnormal Stops Supply Chain Compromise:

Automatically knows your vendors

VendorBase™ auto-identifies suppliers, vendors, and partners via past email conversations and other signals gathered across the enterprise ecosystem.

Continuously monitors vendor risk and reputation

Assigns each vendor a risk score based on domains spoofed, accounts compromised, and suspicious messages.

Examines message content, tone, and attachments

Uses AI and ML to inspect emails and attachments for suspicious signals that can indicate vendor fraud and block the threat from reaching inboxes.

Credential Phishing

Credential phishing attacks are the most common advanced email threat government agencies face. Attackers impersonate trusted parties and well-known brands to steal login credentials to access sensitive data and launch additional attacks.

How Abnormal Stops Credential Phishing:

Inspects email headers to expose impersonations

Determines when an email domain has been spoofed by analyzing header information.

Detects suspicious language, tone, and style

Recognizes the language that indicates phishing attacks, even in messages with no malicious links or attachments.

Understands communication patterns

Applies NLP to understand people's typical tone, behavior, and communication patterns to detect changes that may indicate phishing.

Account Takeover

After a successful credential phishing attack, attackers can use compromised accounts to steal private information about citizens and sensitive public safety data, commit financial fraud, launch ransomware attacks, and more.

How Abnormal Stops Account Takeover:

Determines good sender behavior with multichannel analysis

Leverages API integration with Microsoft 365 and Google Workspace to analyze end-user behavior across devices, browsers, and apps.

Actively monitors user behavior and identity

Detects changes in content and tone, attempts to bypass multi-factor authentication, and shifts in normal login signals, and then auto-remediates suspect accounts.

Includes unique VendorBase™ analysis and monitoring

Baselines known-good interactions with your vendors and evaluates vendor risk scores across the federated database of all customers to understand when a vendor may be compromised and block suspicious emails.

Abnormal

Request Your Abnormal Demo Now:

abnormalsecurity.com/demo →

Proposal Response

Proposal Response

1) Documentation to describe the security operation platform Solution proposed and how it meets the requirements of this RFQ to include the following at a minimum:

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.

Abnormal supports multi-tenancy in the fashion described in the question above. Specifically, Abnormal can support a mix of Google Workspace and Microsoft sub-tenants. Role Based Access Control (RBAC) allows the appropriate permissions and controls to provide aggregated or individual management views.

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.

Content analysis in the form of URLs and attachments is conducted at the time of delivery. This is one of many signals Abnormal will use to condemn a message and render a malicious judgment. The approach taken by Abnormal for high detection efficacy is to remove malicious messages at the time of delivery vs reconstructing a “user safe” version of the message.

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.

Abnormal reviews all emails sent inbound to its customers. If a broader campaign that involves a compromised user is sent internally, Abnormal will analyze and detect the extension of this attack type.

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.

Abnormal can identify a wide range of impersonations (non-spoofed) as well as actual domains that are being spoofed. These impersonations include internal employees, VIPs, and third-party organizations.

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.

URLs are analyzed as one of many detection capabilities at the time of delivery. Using a data science approach, Abnormal can identify novel or zero-day URLs without the use of 3rd party threat intelligence. This capability is available not only within email, but extends into collaboration applications such as Microsoft Teams, Slack, and Zoom.

Abnormal utilizes a sandboxing service which crawls all URLs aside from those associated with phishing simulation campaigns or one-time use URLs (password resets, calendar invites, etc.). The service is architected in such a way where it does not need to be predictive--it will check all URLs found within emails as well as those found within attachments and/or URLs on the landing pages reached via URLs in emails.

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.

URLs and attachments are both examined in a sandbox as part of Abnormal's analysis. Typical checks on both occur (evaluating for behavior of the attachment/landing page, evaluating for common evasive techniques, crawling to identify additional elements [i.e. are there additional URLs at the destination or within the attachment?], crawling as far and wide as possible to evaluate what is contained within), but we also evaluate for behavioral components such as when an email mentions the purpose of the attachment (e.g. “Please view the invoices in the attached”) but the attachment itself is, for instance, a macro-enabled Excel file with all blank cells. These additional checks add another layer to detection similar to our detection for emails more broadly (i.e.. not relying on known bad elements and instead identifying behaviors/attributes that are atypical or abnormal under the circumstances).In addition to the sandboxing, we then incorporate a multitude of other behavior-based checks as it relates to payloads such as: commonality of URL/URL root domain across our dataset (i.e.. all customer environments), commonality of the URL being received in emails within your environment, commonality for emails from the specific sender to contain that specific URL, commonality for emails from the sender to contain a URL with the root domain of the URL, commonality of the URL to be associated with the service mentioned in the email (if relevant)...and a multitude of others. You are able to substitute attachment/attachment type in all of the aforementioned areas I mentioned URLs (commonality of the attachment/attachment type: in general; for the sender; for the recipient; hash/signature; within specific attack types; etc.).This is all also in addition to what essentially amounts to internally generated threat intelligence by which we mean the system can evaluate whether a given URL or attachment (based upon hash/signature) has been seen used in a prior attack in another customer environment.

Microsoft also provides a variety of sandboxing features which may be used in conjunction with Abnormal's sandboxing functionality.

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.

Abnormal leverages machine learning and behavioral AI to detect and stop sophisticated socially-engineered attacks. The platform understands known-good behavior to detect impersonations, changes in invoices or payments, shifts in tone, or other anomalies that may indicate an attack.

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.

Although Real-Time Threat Intelligence has been considered several times within Abnormal from a product development standpoint, Abnormal detection efficacy performs at a superior level to comparable solutions dependent on known threat intelligence - an approach similar to signature-based detection. Using a Data Science based approach, Abnormal can not only detect known phishing attacks and campaigns, but also deliver best in class performance for unknown attacks. Given constant change of payloads to evade threat intelligence, Abnormal is best positioned to detect known and unknown phishing attacks.

Abnormal does employ its own threat intelligence from a campaign classification standpoint. This allows Abnormal to process and learn the attack types and campaigns present in customer environments and is used to classify future attacks.

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.

Abnormal, as well as Microsoft for that matter, are able to use DKIM and DMARC results as a means to aid in threat detection.

The benefit of Abnormal's approach is that hard and fast rules are not all that apply (i.e.. if DMARC is failing then an email must be spoofed). Historical data is considered as well along with other elements of the email to gauge whether an email is actually spoofed or if perhaps a misconfiguration exists on the sender side.

For inbound and outbound DMARC policy configuration, this can be accomplished within Microsoft Exchange Online Protection.

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.

Although User Interface design is a subjective criterion, Abnormal provides an easy to use interface that does not require specialized skill or days worth of training. Customers can typically use the Abnormal portal with proficiency after an hour of training.

Documentation and support resources can be found at support.abnormalsecurity.com.

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.

Abnormal security uses behavioral machine learning (ML) and artificial intelligence (AI) to identify and stop threats. This allows Abnormal to detect every type of attack, including zero-day threats and emails without a malicious payload. This is done by utilizing tens of thousands of signals available via the Microsoft Graph API. Abnormal uses the Microsoft Graph API to scan on receipt. Due to Abnormal's close partnership with Microsoft and a pub/sub API architecture, Abnormal is not susceptible to throttling

6.1.9. Lookalike Domain Detection

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

Abnormal detects the presence of lookalike or typosquat domains. Domain impersonations and lookalikes are provided within the threat analysis of a given attack campaign. An example of this type of attack can be found here.

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.

Abnormal takes the approach to remediate malicious emails that present security risks as opposed to reformatting website content.

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.

Abnormal does not provide URL rewriting. We began developing the functionality but through testing we found that the value-add of such a feature would be almost 0 given the system's performance in detecting and preventing URL-based attacks from reaching users to begin with. Historically URL rewriting has been in place because detection at the time of delivery is not strong enough.

Another consideration here is that URL rewriting is only as good as the solution behind it--in other words, emails with rewritten URLs were deemed safe at the time of delivery so unless there is a swift change in threat intelligence/reputation that URL is still going to be safe at the time of click.

If URL rewriting is still a priority, Microsoft offers URL rewriting and click tracking functionality through their Safe Links functionality.

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.

URLs and attachments are both examined in a sandbox as part of Abnormal's analysis. Typical checks on both occur (evaluating for behavior of the attachment/landing page, evaluating for common evasive techniques, crawling to identify additional elements [i.e.. are there additional URLs at the destination or within the attachment?], crawling as far and wide as possible to evaluate what is contained within), but we also evaluate for behavioral components such as when an email mentions the purpose of the attachment (e.g. “Please view the invoices in the attached”) but the attachment itself is, for instance, a macro-enabled Excel file with all blank cells. These additional checks add another layer to detection similar to our detection for emails more broadly (i.e.. not relying on known bad elements and instead identifying behaviors/attributes that are atypical or abnormal under the circumstances).In addition to the sandboxing, we then incorporate a multitude of other behavior-based checks as it relates to payloads such as: commonality of URL/URL root domain across our dataset (i.e.. all customer environments), commonality of the URL being received in emails within your environment, commonality for emails from the specific sender to contain that specific URL, commonality for emails from the sender to contain a URL with the root domain of the URL, commonality of the URL to be associated with the service mentioned in the email (if relevant)...and a multitude of others. You are able to substitute attachment/attachment type in all of the aforementioned areas I mentioned URLs (commonality of the attachment/attachment type: in general; for the sender; for the recipient; hash/signature; within specific attack types; etc.).This is all also in addition to what essentially amounts to internally generated threat intelligence by which we mean the system can evaluate whether a given URL or attachment (based upon hash/signature) has been seen used in a prior attack in another customer environment.

Microsoft also provides a variety of sandboxing features which may be used in conjunction with Abnormal's sandboxing functionality.

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.

Abnormal currently protects customer environments with hundreds of thousands of mailboxes. Abnormal can scale to the largest organizations globally.

6.1.14. Performance

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

Due to Abnormal’s API approach, mail processing and delivery are not subjected to inline performance based on volume or increased traffic.

6.1.15. Compatibility

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

Abnormal currently integrates with Microsoft 365 and Google Workspace environments.

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.

Given Abnormal’s Data Science approach, the solution does not require, nor have a provision to offer custom configuration. Abnormal customers can take advantage of Safe Lists and Block Lists for explicit permit/deny conditions. Abnormal’s User Interface is easy to use and designed to accommodate users with a range of skill and proficiency levels.

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.

For policy based management, Abnormal recommends utilizing policies within Microsoft Exchange Online Protection.

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).

Abnormal supports Role Based Access Control (RBAC) to manage access to different components within the Abnormal portal. Additionally, Abnormal supports a few different authentication mechanisms: Microsoft SSO (Oauth), GSuite SSO (Oauth), or Okta SSO (SAML). When navigating to a Portal page, a non-logged-in user will be redirected to the login page. Upon entering the email address in question, Portal will redirect to the corresponding authentication service. The authentication service handles authentication and MFA and will redirect back to Portal with attributes about the user and mechanisms to validate the response (e.g. usually a signed token). Once the user is successfully authenticated, Portal will issue out its own signed tokens that satisfy various customer defined requirements (how long a token should last, how much time a user can be inactive, etc.). This token is validated on every request to Portal. What specific product, email, and tenant access a user can have is configurable in the User Management page.

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.

Abnormal recommends configuration of transport rules, content filtering, quarantine and notification settings within Microsoft EOP. Abnormal does support Safe Listing and Block Listing.

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.

Abnormal provides a rich set of reports within its Dashboard as well as the ability to deliver customized reports. Additionally, real time notification for Account Takeovers and Vendor Fraud can be easily configured within the Abnormal Portal.

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.

Abnormal offers a wide range of native integrations to include SIEM providers, XSOAR, Identity. Abnormal and Crowdstrike have developed a bi-directional integration to expose identity based threats. Additionally, customers can use Abnormal's REST API to develop additional custom integrations.

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.

Abnormal offers a wide range of native integrations to include SIEM providers, XSOAR, Identity. Abnormal and Crowdstrike have developed a bi-directional integration to expose identity based threats. Additionally, customers can use Abnormal's REST API to develop additional custom integrations.

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.

In effort to streamline customer requirements for industry standards, compliance, and third-party certification, Abnormal provides customer access to its internal compliance repository known as Security Hub. Within Security Hub, customers can review GDPR, SOC 2, ISO 27001, among many other artifacts. Abnormal will provide access to Security Hub upon request.

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.

Abnormal offers a wide range of native integrations to include SIEM providers, XSOAR, Identity. Abnormal and Crowdstrike have developed a bi-directional integration to expose identity based threats. Additionally, customers can use Abnormal's REST API to develop additional custom integrations.

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).

Abnormal offers a wide range of native integrations to include SIEM providers, XSOAR, Identity. Abnormal and Crowdstrike have developed a bi-directional integration to expose identity based threats. Additionally, customers can use Abnormal's REST API to develop additional custom integrations.

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.

Abnormal natively integrates with Okta and Azure Active Directory. Access to the Abnormal Portal can be controlled through MFA as well.

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.

API integration with The State of Florida and any agencies therein occurs between Abnormal and its Microsoft or Google Workspace tenant. Access to the Abnormal Portal can be controlled in accordance to state policies.

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.

Abnormal will validate proper integration during the time of service delivery. Providing integration occurs using the required permissions, this process is very simple and rarely requires support or maintenance.

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.

The Monthly Availability Percentage for the Service is ninety-nine and nine-tenths percent (99.9%). Please refer to the Abnormal Security Support and Service Level Agreement Policy.

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.

If Service Levels are not met, Abnormal will provide service credits to its customers. Please refer to the Abnormal Security Support and Service Level Agreement Policy.

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.

Acknowledged and agreed to by Abnormal.

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.

Training on Abnormal's platform is provided at no cost. Training is conducted through a web conferencing session (Zoom, Webex, etc.).

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).

Not Applicable

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.

Not Applicable

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.

Support response times are listed in Table 1 within the Support and Service Level Agreement Policy.

6.3. Kickoff Meeting

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

Abnormal provides a structured kickoff meeting to clarify expectations as a standard business practice.

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.

Abnormal provides a structured kickoff meeting to clarify expectations as a standard business practice. This extends to multiple customers and agencies.

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.

Abnormal will provide a demonstration of its solution to any customer stakeholder during or before any scheduled kickoffs.

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.

Implementation will predominantly fall under the responsibility of Abnormal Security. Tasks involved are communicated to each customer before service integration. Customer tasks are typically limited to creating additional portal accounts and permissions. Abnormal will ask for specific details on existing Security Awareness Training and providers for internal phishing campaigns in effort to allow these messages to be delivered.

6.4.2. Identify if the Contractor, Purchaser, FL[DS] (if applicable), or other Customer is responsible for each task.

Abnormal will assign a Customer Success Manager and Delivery Manager as Directly Responsible Individuals (DRI) for service delivery.

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.

Service delivery is accomplished within about an hour of time. Abnormal will provide a timeline of key milestones and dates for service delivery.

6.4.4. Describe necessary training, method of training (e.g., in-person, live webinar, online course), and training dates.

Training is conducted virtually through the use of tools such as Zoom, Webex, or equivalent. Training dates are subject to Abnormal and customer availability. Training will include a comprehensive overview of the Abnormal portal.

6.4.5. Describe the support available to ensure successful implementation and Initial Integration.

Abnormal is directly responsible for a successful implementation and Initial Integration. Customer support is not typically required as provisioning and deployment tasks are handled by Abnormal.

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.

All DRI contact information will be provided during our Customer Kickoff and Onboarding sessions.

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.

Implementation is completed in a single session, typically an hour of time. Ongoing implementation beyond one session is highly atypical. Abnormal will communicate in a manner and frequency that satisfies customer requirements.

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.

Abnormal provides QBRs to its customers as a standard business practice. This includes attack reviews, metrics, roadmap items, and any key areas of interest stated by the customer.

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.

Upon initial integration of Abnormal service, there is no further or ongoing implementation with the exception of any subtenants added to the customer environment. In scenarios where customers expand or add subtenants, Abnormal will use the same process for onboarding and implementation as described within this document. If necessary, Abnormal can address expansion status during QBRs.

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.

Training is provided at the time of service delivery. If necessary, Abnormal can include training topics and attendees during QBRs.

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.

Abnormal will provide the requested items during QBRs.

6.5.5. Ad hoc reports as requested by the Purchaser.

Acknowledged by Abnormal.

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.

Acknowledged by Abnormal. Any additional services and pricing will be presented to the customer.

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.

Abnormal will review any proposed SLAs involving future integrations. This may be subject to legal agreements between both parties.

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.

Abnormal will review any proposed SLAs involving future integrations. This may be subject to legal agreements between both parties.

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

Please see the attached.

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

Please see the attached.

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).

Optiv’s proposed pricing meets this requirement.

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

Please see the response below.

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

Please see the attached.

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

Please see the attached.

f. A draft disaster recovery plan per section 32.5.

Please see the attached.

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

Abnormal has significant experience providing this solution to government organizations with over 900,000 managed government inboxes.

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

There is no limitation on our ability to implement the solution on a statewide basis.

4) Detail regarding any value-added services.

Please see the response below.

Abnormal

Protect Grant Funding

Secure your federal funding from the full spectrum of cyberattacks with a robust cloud-native solution.

Federal financial assistance, primarily administered as grants, is one of the most significant sources of funding for state, local, and tribal governments, as well as educational institutions across K-12 school districts, colleges, and universities. Most often, federal grants are awarded as direct cash assistance, but federal grants can also include in-kind assistance.

There is an estimated **$1 trillion** in outlays for aid to state, local, tribal, and territorial governments in 2023. Unfortunately, these funds are prime targets for bad actors to attempt to steal. The ever-changing landscape of business email compromise (BEC) accounts for more financial loss than any other cyberthreat—and the media attention resulting from these grants enables threat actors to obtain all the information they need to target employees with socially-engineered attacks.

There is little denying that government employees and grantees play a key role in preventing fraud related to taxpayer-funded programs.

Email-Like Attacks Targeting Your Funding

Cybersecurity risks in grant funding pose a significant threat to organizations and individuals alike. Cybercriminals often target grant funding as a source of money, knowing that grant administrators may not have the same level of security in place as traditional banking institutions.

Cyberattackers may use a variety of methods to gain access to grant funds, such as phishing, malware, or social engineering techniques. These attacks can lead to a loss of funds, disruption of services, increased risk of data breaches, and reputation damage to the grant recipient. It is crucial that grant administrators take the necessary steps to protect their funds from cyber threats.

Recently there have been numerous accounts of Local Governments suffering attacks targeting Federal Funds for such things as Housing and Rental Assistance, COVID funding, ARPA funding, and others.

In light of these threats, many organizations are turning to Abnormal Security to safeguard their federal financial funds. Abnormal offers a robust cloud-native security solution so you can prevent email and email-like attacks that target your grant funding, while automating your security operations.

$1.2 Trillion

Issued in federal financial assistance to state, local, tribal, and territorial governments in 2022.

**Grants.gov*

175%

Increase in BEC attack volume between over the last years.

**Abnormal Research*

$2.7 Billion

Lost to BEC attacks in 2022 alone.

**FBI Internet Crime Center (IC3)*

Abnormal Keeps Your Grant Funding Secure from Email Threats Aiming to Steal It

Baselines known good behavior across employees, vendors, and partners by analyzing every email from every identity across thousands of contextual signals, to build risk-aware detection models and stop all types of inbound email attacks.

Automatically builds searchable knowledge engines with detailed profiles of your organization's employees and vendors and monitors their risk levels.

Remediates malicious emails to a hidden folder within milliseconds, removing the possibility of end user engagement.

Fully automates email triage, remediation, and reporting, bringing together all auto-detected and user-reported threats into a single interface.

Helps employees and executives be more productive by automatically moving unwanted mail out of the inbox.

See Abnormal in Action. **Request a Demo.**

abnormalsecurity.com →

Abnormal for Grant Funding

Stop the most dangerous attacks that bypass your existing defenses.

Supply Chain Compromise

When your vendors ore compromised, you con be compromised too. Attackers who breach trusted vendor email accounts can send fraudulent invoices and credential phishing attacks that bypass your security systems.

How Abnormal Stops Supply Chain Compromise:

Automatically knows your vendors

VendorBase™ auto-identifies suppliers, vendors, and partners via past email conversations and other signals gathered across the entire ecosystem.

Continuously monitors vendor risk and reputation

Assigns each vendor a risk score based on domains spoofed, accounts compromised, and suspicious messages.

Examines message content, tone, and attachments

Uses AI and ML to inspect emails and attachments for suspicious signals that can indicate vendor fraud and block the threat from reaching inboxes.

Credential Phishing

Attackers can spoof the internal email addresses of instructors or administrators to steal login IDs and passwords from students or staff, which they can then leverage to launch more damaging attacks.

How Abnormal Stops Credential Phishing:

Inspects email headers to expose impersonations

Determines when an email domain hos been spoofed by analyzing header information.

Detects suspicious language, tone, and style

Recognizes the language that indicates phishing attacks. even in messages with no malicious links or attachments.

Understands communication patterns

Applies natural language processing (NLP)to learn people's typical tone, behavior, and communication patterns to detect changes that mayindicate phishing.

(D

Account Takeover

The FBI notified colleges and universities in May 2022 about a growing number of stolen academic credentials for sale online. Similar to this. criminals can use these credentials to access internal systems and steal or ransom sensitive data.

How Abnormal Stops Account Takeover:

Determines goad sender behavior with multichannel analysis

Leverages API integration with Microsoft 365 and Google Workspace to analyze end-user behavior across devices, browsers, and opps.

Actively monitors user behavior and identity

Detects changes in content and tone, attempts to bypass multi-factor authentication. and shifts in normal login signals and then auto-remediates suspect accounts.

Includes unique VandorBase"' analysis and monitoring

Baselines known-good interactions with your vendors and evaluates vendor risk scores across the federated database of all customers to understand when a vendor may be compromised and block suspicious emails.

[gJ

Ransomware

Ransomware candisrupt classes, expose student data,and even cause schools to permanently close. Socially-engineered emails can trick students or staffers into giving credentials to attackers, who then access and encrypt critical systems.

How Abnormal Stops Ransomware:

Analyzes message content and other signals for credential phlshing

Utilizes identity detection and NLP to spot first-stage attacks **like phishing, even when messages come from trusted senders.**

Blocks malicious attachments and links

Reviews all attachments and links for safety, including links that redirect upon clicking.

Gives security teams explainable insights and **malware forensics**

Automatically prepares detailed analyses of ransomwore attempts, enabling teams to preview attachment content and link targets.

Attachment A - Price Sheet

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***

__X__ ***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)

Decline to respond

IV. Pricing - Integrated Cloud Email Security (ICES))

Initial Term Pricing (Years 1-3)		
Item No.	**Description**	**Rate Per Device**
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	$ 35.40 (waterfall discounting schedule found below)

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	$ 35.40 (waterfall discounting schedule found below)

Please note: This is a 5% uplift on renewals if there is not a multi-year deal in place. If the customer commits to a multi-year deal, the price stays flat (no 5% uplift).

Optional Renewal Term Pricing (Years 4-6)		
Item No.	**Description**	**Rate Per Device**
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	$ 37.17 (waterfall discounting schedule found below)
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	$ 37.17 (waterfall discounting schedule found below)

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 (including implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
IES - M	**Inbound Email Security for Microsoft Office 365 (licensed per mailbox)**	**$106.24**	**$25.00**
ATO - M	**Email Account Takeover Protection for Microsoft Office 365 (licensed per**	**$31.40**	**$5.20**

	mailbox)		
AMX - M	**Abuse Mailbox Automation for Microsoft Office 365 (licensed per mailbox)**	**$31.40**	**$5.20**
IES - G	**Inbound Email Security for Google Workspace (licensed per mailbox)**	**$106.24**	**$25.00**
ATO - G	**Email Account Takeover Protection for Google Workspace (licensed per mailbox)**	**$31.40**	**$5.20**
AMX - G	**Abuse Mailbox Automation for Google Workspace (licensed per mailbox)**	**$31.40**	**$5.20**

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	**SKU Description**	**Market Price**	**ACS Price**
IES - M	**Inbound Email Security for Microsoft Office 365 (licensed per mailbox)**	**$106.24**	**$25.00**
ATO - M	**Email Account Takeover Protection for Microsoft Office 365 (licensed per mailbox)**	**$31.40**	**$5.20**
AMX - M	**Abuse Mailbox Automation for Microsoft Office 365 (licensed per mailbox)**	**$31.40**	**$5.20**
IES - G	**Inbound Email Security for Google Workspace (licensed per mailbox)**	**$106.24**	**$25.00**
ATO - G	**Email Account Takeover Protection for Google Workspace (licensed per mailbox)**	**$31.40**	**$5.20**
AMX - G	**Abuse Mailbox Automation for Google Workspace (licensed per mailbox)**	**$31.40**	**$5.20**

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.

Mailbox Size	**Price per mailbox**	**Term**
1-999	$35.40	1 year
1000 - 9999	$24.20	1 year
10,000 - 99,999	$15.40	1 year
100,000+	$9.80	1 year

			FL Tier 1	FL Tier 2	FL Tier 3	FL Tier 4
	LIST		1-999 mbx	1000-9999 mbx	10000-99999 mbx	100000+ mbx
IES	$106.24		$25.00	$15.00	$10.00	$8.00
ATO	$31.40		$5.20	$4.60	$2.70	$0.90
AMX	$31.40		$5.20	$4.60	$2.70	$0.90
			$35.40	**$24.20**	**$15.40**	**$9.80**

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.

Not available.

VII. Value-Added Services (Optional)

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

Not available.

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.

Optiv Security Inc.	DocuSigned by: Jacquelyn Wayne 381FC9E99088435...
Vendor Name	***Signature***
43-1806449	Jacquelyn Wayne
FEIN	***Signatory Printed Name*** BL
May 24th, 2023	
Date	

Attachment B - Contact Information Sheet

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:	Ed Topoleski	Ed Topoleski
Title:	Client Manager	Client Manager
Address (Line 1):	500 N. Westshore Blvd.	500 N. Westshore Blvd.
Address (Line 2):	Suite 950	Suite 950
City, State, Zip Code	Tampa FL 33609	Tampa FL 33609
Telephone (Office):	(321) 277-1398	(321) 277-1398
Telephone (Mobile):	(321) 277-1398	(321) 277-1398
Email:	Ed.Topoleski@optiv.com	Ed.Topoleski@optiv.com

Non-Disclosure Agreement

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

Optiv Security Inc.

This Confidentiality and Non-Disclosure Agreement ("Agreement") is between the Florida Department of Management Services ("Department"), a state agency, and Optiv Security Inc. ("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) <u>Access</u>: 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) <u>Affiliates</u>: Any agents, affiliates, partners, subcontractors, resellers, distributors, dealers, or other entities associated with Recipient that have Access to the Confidential Data.
   (c) <u>Agreement-related Materials</u>: Materials created or provided by Recipient while performing the Agreement.
   (d) <u>Confidential Information</u>: 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	**Optiv Security Inc.**
By: ______________________	DocuSigned by: By: Jacquelyn Wayne 381FC9E99088435...
Name: ______________________	Name: Jacquelyn Wayne
Title: ______________________	Title: SVP & Associate General Counsel
Date: ______________________	Date: May 24th, 2023

BL

Optiv Overview

Optiv Overview

Optiv is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. We employ our real-world experience, deep vertical expertise, diverse teams and proven best practices to drive products, programs and leadership to attack any challenge.

Optiv is backed by the full financial strength of investors like KKR and Blackstone. Our leadership team are pioneers with cutting-edge business and cybersecurity experience and the board of directors bring decades of combined experience in cybersecurity, global threat intelligence insight and building innovative companies and brands. Members include John Park, KKR partner and leader of the KKR technology industry team; Dave DeWalt, NightDragon founder and CEO and former McAfee CEO and FireEye founder; retired U.S. Army General David Petraeus, KKR partner and chairman of the KKR Global Institute; and Blair Christie, former CISCO chief marketing officer.

Optiv's comprehensive ecosystem of hardware and software manufacturers includes more than 600 partners. We are continuously innovating and transforming the cybersecurity delivery and consumption model, which allows Optiv to reduce complexity and remove the symptoms that are roadblocks to business innovation.

7,000+
Clients served in more than 65 countries

~$3B
2021 sales

2,300
Employees, including ~1,600 cybersecurity experts

1,100
Field staff dedicated to client success

600
Technology partners

3,000
Technology certifications

24/7/365
SOC coverage around the world

Optiv employees are instrumental in driving the security industry forward and we care deeply about the communities where we live and work. That passion to make our world and communities a better and more equitable and inclusive place fuels Optiv Chips In, our corporate social responsibility initiative, and Optiv's Diversity Equity and Inclusion (DE&I) program. Through these efforts, we collectively give our time and money to dozens of philanthropic projects with organizations like local food banks, Foster Adopt Connect, Boys and Girls Club and many more. This program spotlights the experience of many service members employed at Optiv.

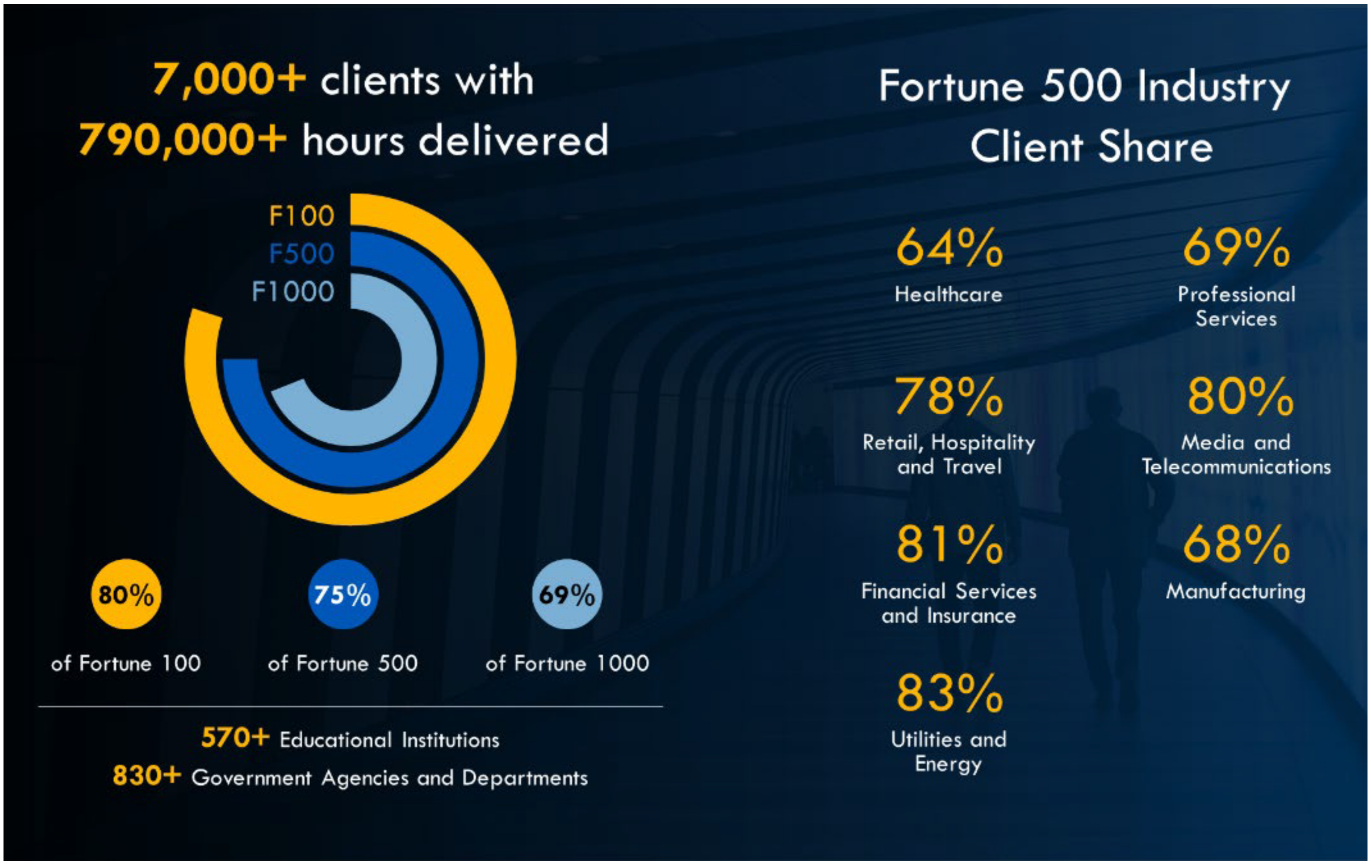
We also honor and embrace the diverse perspectives, ideas, backgrounds and experiences of our people. This unwavering commitment is a key element of our company values and core to who we are and how we operate. When we feel recognized, represented and respected, we do our best work and create the greatest value for our clients. Our approach to DE&I is grounded in listening, learning and growing with a focus on Optiv Women's Network, Optiv Black Employee Network, Pride and Optiv Veterans.

Built on decades of consistent vision and measured growth, Optiv is structured to successfully partner with businesses of every size and industry from Fortune 500 enterprises to smaller county governments and local businesses. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential. No matter where you are on your cybersecurity journey, we stand ready to help.

Partner Ecosystem

A10
Accellion
ACCESSDATA
Aerohive
Agiliance
airwatch
ARBOR
ARISTA
Barracuda
BeyondTrust
BITSIGHT
BlackBerry CYLANCE
BRADFORD NETWORKS
BROCADE
BLUECAT
Centrify
CROWDSTRIKE
COFENSE
DAMBALLA
DIGITAL GUARDIAN
endace
Entrust
ExtraHop
Fidelis
gemalto
GUIDANCE
invincea
LIEBERMAN SOFTWARE
LockPath
loglogic
MICRO FOCUS
aruba
BLUE COAT
Check Point
CISCO
CYBERARK
f5
FIREMON
FIREEYE
Forcepoint
FORESCOUT
FORTINET
Gigamon
Hewlett Packard Enterprise
IBM Security
Infoblox
imperva
ixia
JUNIPER
LogRhythm
McAfee
paloalto
proofpoint
Qualys
RSA
splunk
Symantec
TANIUM
TREND MICRO
vmware Carbon Black
mobileiron
NETSCOUT
netskope
NORSE
onapsis
okta
Ping Identity
radware
RAPID7
REDSEAL
riverbed
SailPoint
SECUREAUTH
Security Compass
SKYBOX
skyhigh
solarwinds
SOPHOS
tenable
THALES
tufin
tripwire
VARONIS
VENAFI
VERACODE
VSS Monitoring
WhiteHat
zscaler
WatchDox

Who We Serve



7,000+ clients with
790,000+ hours delivered

80% of Fortune 100

75% of Fortune 500

69% of Fortune 1000

570+ Educational Institutions
830+ Government Agencies and Departments

Fortune 500 Industry Client Share

64% Healthcare	69% Professional Services
78% Retail, Hospitality and Travel	80% Media and Telecommunications
81% Financial Services and Insurance	68% Manufacturing
83% Utilities and Energy	

Optiv Industry Awards

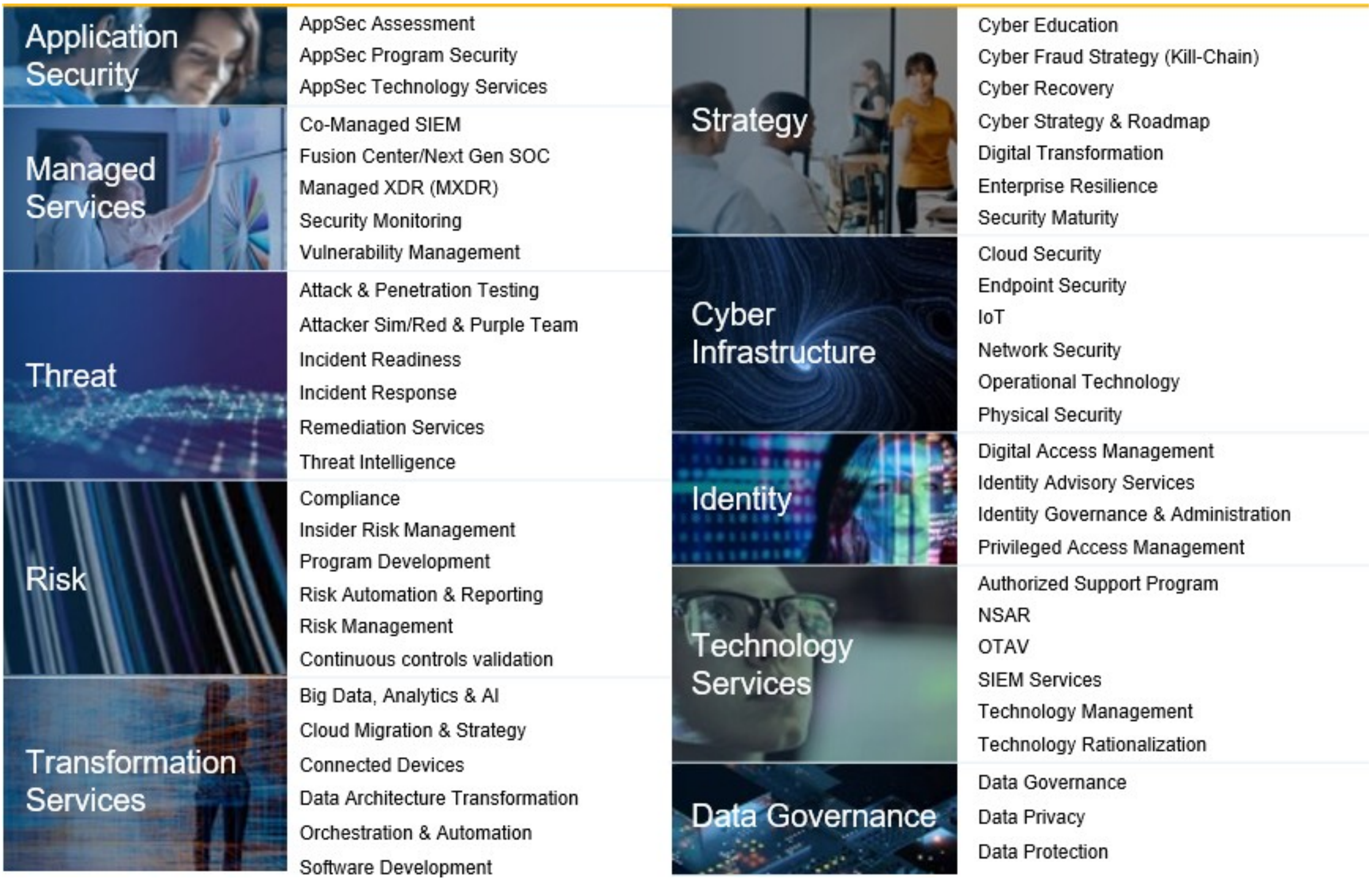
Optiv is consistently recognized in reports from analyst firms such as a **Gartner** and **Forrester** for our end-to-end capability and scale in Security Consulting and MSS.

Optiv has been named as a Representative Vendor in Gartner’s 2022 Market Guide for Managed Security Information and Event Management, Gartner’s 2022 Market Guide for Managed Security Services and Gartner’s 2021 Market Guide for Managed Detection and Response Services.

Optiv is also listed in Forrester’s Now Tech for Global Cybersecurity Consulting Providers for Q3 2021 and ranked as the number one pure-play security company in CRN’s 2021 Solution Provider 500.

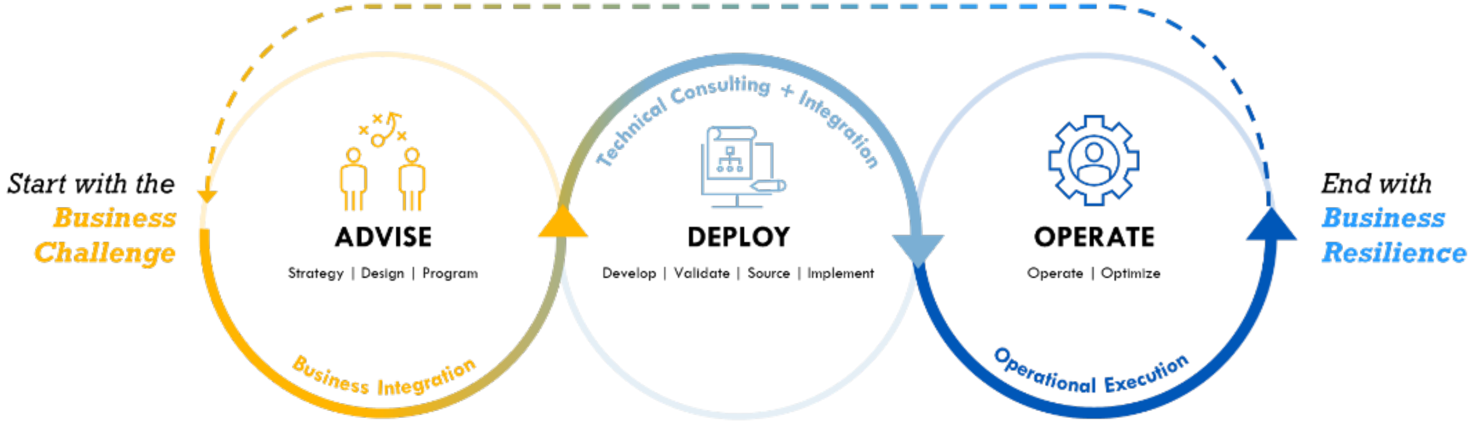
Historically, Optiv is consistently ranked as a top 10 Global Security Consultant and a top 20 global MSSP.

Comprehensive Suite of Cybersecurity Services



Application Security	AppSec Assessment AppSec Program Security AppSec Technology Services
Managed Services	Co-Managed SIEM Fusion Center/Next Gen SOC Managed XDR (MXDR) Security Monitoring Vulnerability Management
Threat	Attack & Penetration Testing Attacker Sim/Red & Purple Team Incident Readiness Incident Response Remediation Services Threat Intelligence
Risk	Compliance Insider Risk Management Program Development Risk Automation & Reporting Risk Management Continuous controls validation
Transformation Services	Big Data, Analytics & AI Cloud Migration & Strategy Connected Devices Data Architecture Transformation Orchestration & Automation Software Development
Strategy	Cyber Education Cyber Fraud Strategy (Kill-Chain) Cyber Recovery Cyber Strategy & Roadmap Digital Transformation Enterprise Resilience Security Maturity
Cyber Infrastructure	Cloud Security Endpoint Security IoT Network Security Operational Technology Physical Security
Identity	Digital Access Management Identity Advisory Services Identity Governance & Administration Privileged Access Management
Technology Services	Authorized Support Program NSAR OTAV SIEM Services Technology Management Technology Rationalization
Data Governance	Data Governance Data Privacy Data Protection

Continuous Security Solutions Support



Start with the **Business Challenge**

ADVISE
Strategy | Design | Program
Business Integration

Technical Consulting + Integration

DEPLOY
Develop | Validate | Source | Implement

OPERATE
Operate | Optimize
Operational Execution

End with **Business Resilience**

OPTIV

Secure greatness™

Optiv Security is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential.

Abnormal Security Implementation, Support, and Training Resources

Overview

Onboarding

We will need details on your onboarding preferences to customize your enablement.

Product Updates and Feedback

Use the Suppo rt Portal to learn about feature enhancements and leverage your CSM and AE/account team for feedback, quick questions

Quarterly Business Reviews

We will meet periodically to discuss your initiatives/business updates, discuss your threat landscape, trends, product feedback, sync on our shared goals, and make any modifications needed to keep us working better together.

Getting Answers For Issues

Open Support Cases

Your Abnormal Security Project Team

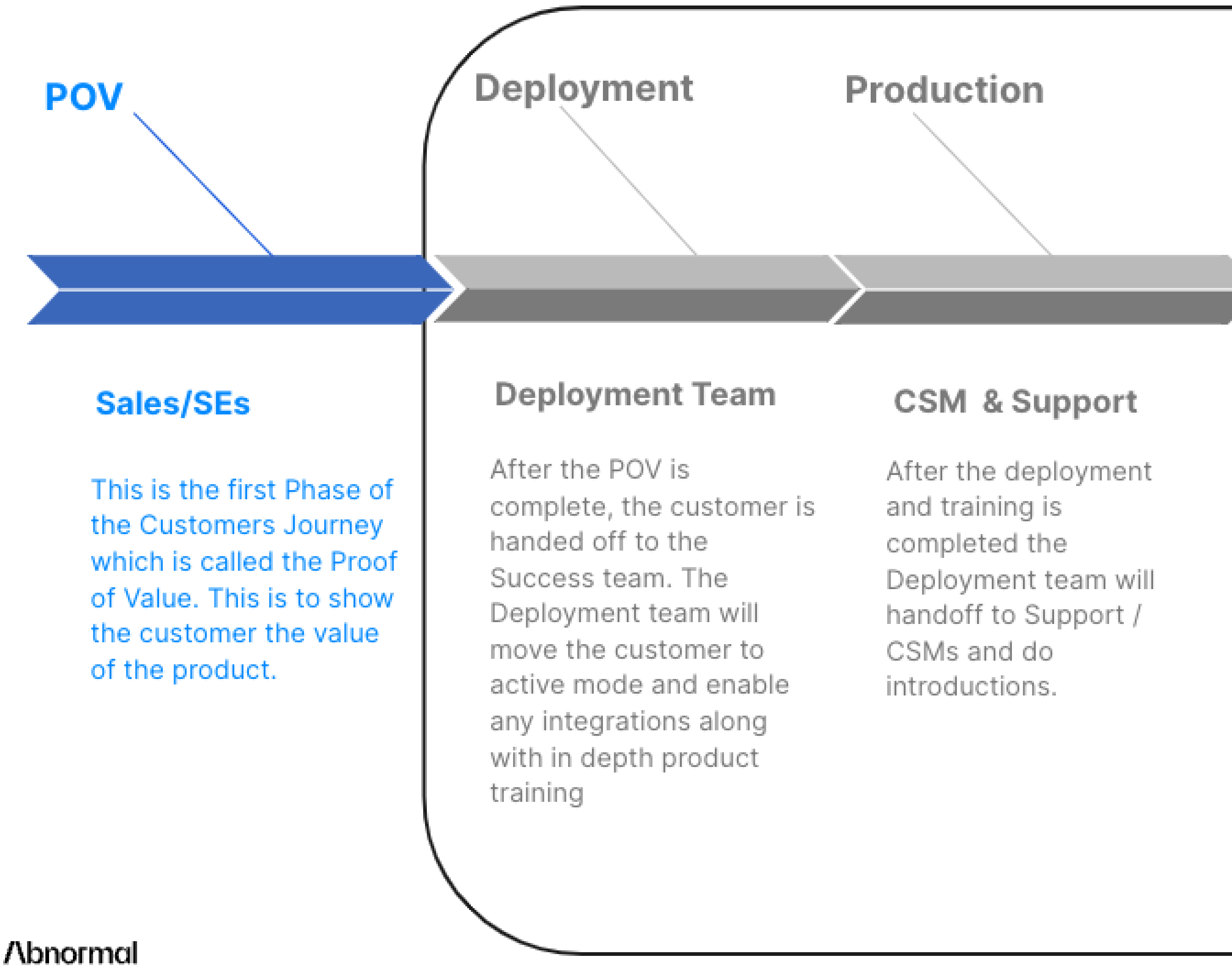
- Deployment Engineer -
  - Primary technical point of contact during implementation.
- Customer Success Manager -
  - Responsible for Abnormal account relationship post-implementation.
- Head of Customer Success and Support
  - Responsible for Customer Success at Abnormal Security.
- Support Portal - support@abnormalsecurity.com
  - Contact the Support Team to troubleshoot and resolve technical issues with Abnormal products.
- Account Executive -
  - Responsible for overall relationship between our companies

Abnormal Roles Overview

Role	Overview
Deployment	● Deployment of product ● Support Customer during deployment ● Customer Training and Support ● Initial Customer Feedback ● Custom Configuration

Customer Success Manager (CSM)	● Adoption ● Quarterly Business Reviews ● Regular Customer Sync ● Working with AEs on Renewals ● troubleshooting, analyze and escalate issues to supp
Support Engineer	● First response and triage for cases/issues ● Break-fix case handling ● Manage Salesforce Backlog ● Able to propose solutions and/or debug ● Incident handling and communication ● Manage Jira and Salesforce Backlog
Enablement	● Creates customer facing and internal documentation ● Creates CSS Onboarding/Training ● Works with Prod/Marketing on Incident Comms ● Develops templates

Customer Success and Support



POV

Sales/SEs

This is the first Phase of the Customers Journey which is called the Proof of Value. This is to show the customer the value of the product.

Deployment

Deployment Team

After the POV is complete, the customer is handed off to the Success team. The Deployment team will move the customer to active mode and enable any integrations along with in depth product training

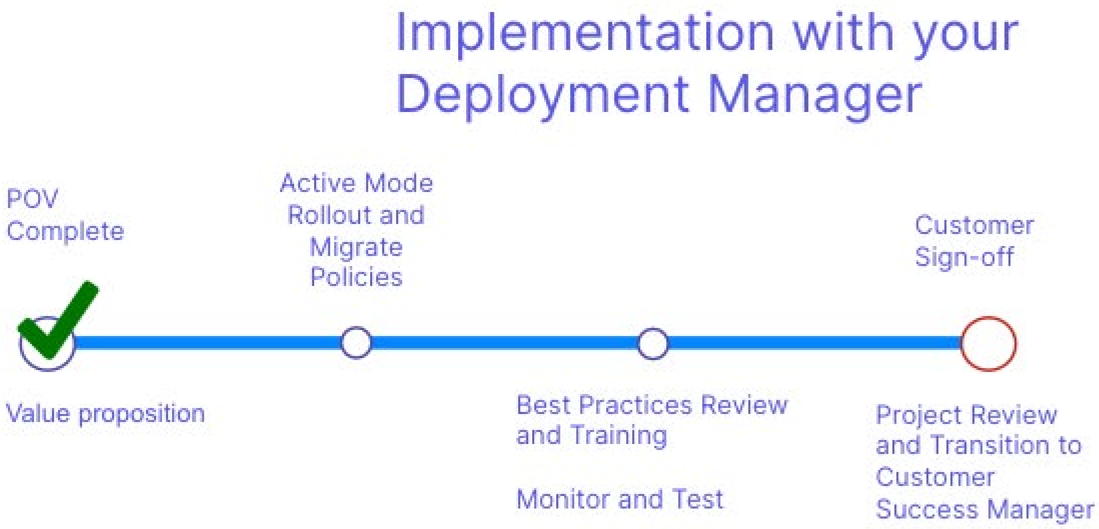
Production

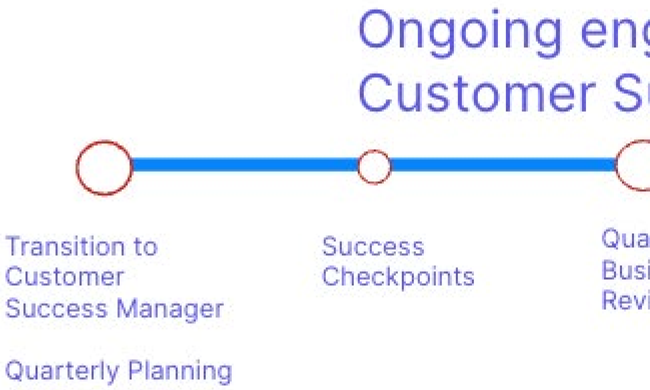
CSM & Support

After the deployment and training is completed the Deployment team will handoff to Support / CSMs and do introductions.

Abnormal

Abnormal Implementation Overview


Implementation with your Deployment Manager
POV Complete
Active Mode Rollout and Migrate Policies
Customer Sign-off
Value proposition
Best Practices Review and Training
Monitor and Test
Project Review and Transition to Customer Success Manager



Severities and SLAs

Severity	Description	Response	Examples	Cust
1 (Urgent)	System Down. Complete failure of the software, impacting all users. Incident is causing a service disruption for	1 hour	● Email Detection and Remediation failing ● Portal offline along with	Comm availa neede apply

	production users or a degrading condition that renders the service inoperable.		Email analysis degradation	
2 (High)	The software is operating in degraded mode. One or more of the subsystems is not functioning or impacting only a subset of the users. Incident is causing a service degrading condition, but the service is still operable.	2 hours	● Portal Offline or intermittent failure ● Internal Account takeover not detected ● Link Analysis and attachment detonation services degraded	Comm availa neede apply
3 (Normal)	All major functionality is working. Non-critical system issues. The service is running with limited functionality in one or more subsystems or intermittent issues	8 hours	● False Positives ● False Negatives ● How to Question	Monit
4 (Low)	How-To Questions and software issues with no degradation.	24 hours	● Third party integration setup ● Cosmetic bugs in the GUI	Monit
RFE	Requests for Enhancement	2 days	● Reporting enhancements ● Search functionality enhancements	N/A

Support Resources

Email: support@abnormalsecurity.com

Phone:

APAC	+61-2-7202-1574
EMEA	+44-330-818-7426
US	+1-866-466-9321
Direct	+1-415-326-1372

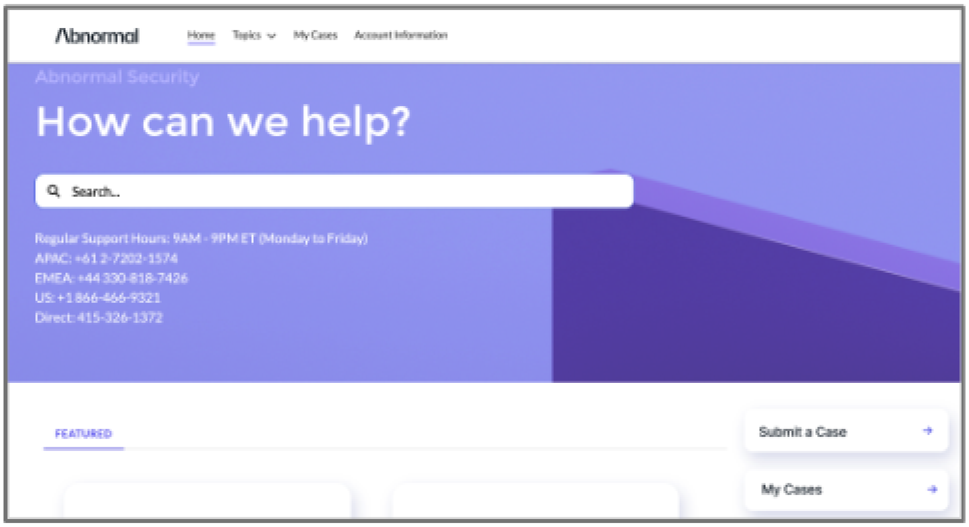
Business Hours:

24/5 - Monday to Friday
24/7 - Severity 1 Support

Login to the Support Portal

Submit Cases and Search for Knowledge

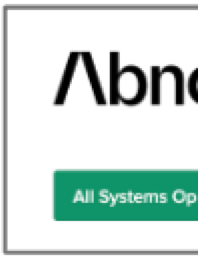
https://support.abnormalsecurity.com



How can we help?

Regular Support Hours: 9AM - 9PM ET (Monday to Friday)
APAC: +61 2-7202-1574
EMEA: +44 330-818-7426
US: +1 866-466-9321
Direct: 415-326-1372

Status Page:
Sign up
availabil
https://a



You can Sign
texts),

Intro

- Customer S
  - How to
    informat
- Best Practic
  - Abnorma

Abnormal Academy - Training Portal

- Access to on-demand training, customized to your specific deployment needs
- Guides to the Portal, Dashboard, and other tools Abnormal provides
- Badges for completing customized paths and *Abnormally Certified Essentials* Certification, both of which are shareable on LinkedIn

Register at https://abnormal-academy.workramp.io

Community : Abnormal Inspired

- Contact your peers to talk about Abnormal and how you use it.
- The Support Team is one of the moderators to keep things running smoothly and answer any questions the Community struggles with.

Abnormal Intelligence: Insight into Emerging Attacks

- Discover the latest information about email threats and new attacks to keep your organization safe from cybercrime.

Trust Center: Security and compliance information

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

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

Optiv Security Inc.

This Confidentiality and Non-Disclosure Agreement ("Agreement") is between the Florida Department of Management Services ("Department"), a state agency, and Optiv Security Inc. ("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	**Optiv Security Inc.**
By: DocuSigned by: Pedro Allende 5E91A9D369EB47C...	By: DocuSigned by: Jacquelyn Wayne 381FC9E99088435...
Name: Pedro Allende	Name: Jacquelyn Wayne
Title: Secretary	Title: SVP & Associate General Counsel
Date: 6/14/2023 | 5:00 PM EDT	Date: May 24th, 2023

BL