

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

---

**AGENCY TERM CONTRACT  
FOR  
Security Operations Platform  
DMS-22/23 157C  
BETWEEN  
STATE OF FLORIDA  
DEPARTMENT OF MANAGEMENT SERVICES  
AND  
INSIGHT PUBLIC SECTOR, 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 INSIGHT PUBLIC SECTOR, INC. (Contractor), with offices at 2701 E Insight Way, Chandler, AZ 85250, 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-22/23-157, Security Operations Platform; 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-22/23-157.

**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-22/23-157.
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-22/23-157 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](mailto: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](mailto: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:

Stephen Forsythe  
Client Executive  
2701 E Insight Way  
Chandler, AZ 85250  
Telephone: (850) 428-7966  
Email: [Stephen.Forsythe@Insight.com](mailto:Stephen.Forsythe@Insight.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

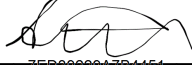
During the term of the Contract, Contractor shall not knowingly employ, subcontract with or subgrant to any person (including any non-governmental entity in which such person has any employment or other material interest as defined by section 112.312(15), F.S.) who is employed by the State or who has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

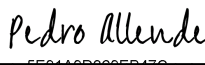
**SIGNATURE PAGE IMMEDIATELY FOLLOWS**

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

INSIGHT PUBLIC SECTOR, INC:

STATE OF FLORIDA  
DEPARTMENT OF MANAGEMENT SERVICES:

DocuSigned by:  
  
7ED39229A7B4451...  
Authorized Signature

DocuSigned by:  
  
5E91A9D309EB47C...  
Pedro Allende, Secretary

Scott Friedlander  
Print Name

6/30/2023 | 8:03 PM EDT  
Date

Insight Public Senior Vice President  
Title

6/30/2023 | 5:02 PM PDT  
Date

**Exhibit "A"**  
**Request for Quotes (RFQ)**  
**DMS-22/23-157**  
**Security Operations Platform 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 Extended Detection and Response (XDR) platform, which is a platform that combines multiple security technologies and tools, such as EDR (Endpoint Detection and



Response), NDR (Network Detection and Response), and SIEM (Security Information and Event Management), into a single, integrated platform.

## **2.0 OBJECTIVE**

Pursuant to section 287.056(2), F.S., the Department intends to purchase a security operations platform Solution for use by the Department and Customers to combine multiple security technologies and tools, such as EDR, NDR, and SIEM, into a single, integrated platform 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 a security operations platform 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 combine multiple security technologies and tools into a single integrated platform. The Solution must be designed to provide a comprehensive view of security posture, by consolidating security data from across the entire IT infrastructure. This enables security teams to quickly detect, investigate, and respond to security threats, with the goal of minimizing the impact of security incidents and reducing overall risk. In addition to integrating multiple security technologies, extended detection and response platforms typically leverage AI and machine learning to analyze large volumes of security data and automate threat detection and response processes. This can help reduce the burden on security teams and improve the speed and accuracy of security operations.

#### **6.1.1. Multi-Tenant**

The Solution shall support a multi-tenant architecture, allowing multiple organizations or departments to securely and independently operate within the same system, with separate data storage and access controls. Each tenant shall have its own instance and each instance should aggregate up to a single instance and view, allowing for enterprise-wide visibility into threats, investigations, and trends. The Solution shall also provide dashboards for single source visibility into incidents and response activities across all tenants.

#### **6.1.2. Detection and Response**

The Solution shall have the ability to detect and respond to a wide range of security threats, including malware, phishing, insider threats, and zero-day attacks.

### **6.1.3. Scalability**

The Solution shall be scalable to meet the needs of organizations of all sizes, from small businesses to large enterprises. The Solution shall have the ability to handle a high volume of events and alerts while maintaining performance and accuracy.

### **6.1.4. Automation**

The Solution shall have the ability to automate responses to threats, including containment, isolation, and remediation.

### **6.1.5. Incident Reporting**

The Solution shall provide detailed reporting on security incidents, including alerts, investigations, and remediation activities.

### **6.1.6. User Management**

The Solution shall have a robust user management system that allows administrators to control access to the platform, set permissions, and manage user accounts.

### **6.1.7. Cloud Deployment**

The Solution shall be deployable in a cloud environment and should support multi-cloud deployments.

### **6.1.8. Threat Intelligence**

The Solution shall leverage threat intelligence to provide contextual information about threats and enable faster, more accurate response.

### **6.1.9. Incident Response**

The Solution shall support incident response workflows, including playbooks and case management, to enable efficient and effective response to security incidents.

### **6.1.10. Data Management and Storage**

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

#### **6.1.11. Performance Management**

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

#### **6.1.12. Disaster Recovery and Backup**

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

#### **6.1.13. Identity and Access Management**

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

#### **6.1.14. Network**

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

#### **6.1.15. 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.

#### **6.1.16. Integration**

**6.1.16.1.** The Solution shall integrate with the Department's existing security tools such as firewalls, antivirus software, and 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.

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

**6.1.16.3.** 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.

**6.1.16.4.** 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.

**6.1.17. 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.

**6.1.17.1.** 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.

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

**6.5. Reporting**

The Contractor shall provide the following reports to the Purchaser:

- 6.5.1. Quarterly Business Reviews (QBR) which will include, but not be limited to, performance reports and metrics on service level achievements. The Contractor shall schedule a quarterly meeting to review the QBR and document any financial consequences to be assessed as necessary.
- 6.5.2. Monthly Implementation Reports shall be provided to the Purchaser to document compliance with Final Implementation Plan(s) and document any financial consequences to be assessed as necessary.
- 6.5.3. Monthly Training Reports shall be provided to the Purchaser to document all training provided to the Purchaser and any other Customers and document any financial consequences to be assessed as necessary.
- 6.5.4. Monthly Service Reports shall be provided to the Purchaser to document Solution performance, availability, response times, and resolution times and document any financial consequences to be assessed as necessary.
- 6.5.5. Ad hoc reports as requested by the Purchaser.

**6.6. Optional Services**

**6.6.1. Manage, Detect, and Respond (MDR)**

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

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

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

**6.6.2. Future Integrations**

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

6.6.2.1. Adhere to the FL[DS]-approved SLA for future integrations which include services and solutions that augment, enhance, or expand the Solution in a meaningful way.

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

**7.0 DELIVERABLES**

Deliverables for each Purchase Order may be submitted earlier than the delivery dates listed in **Table 1**. All deliverables are subject to the approval and acceptance of the Purchaser. The

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

<b>TABLE 1 DELIVERABLES AND FINANCIAL CONSEQUENCES</b>			
<b>No.</b>	<b>Deliverable</b>	<b>Time Frame</b>	<b>Financial Consequences</b>
1	The Contractor shall host a kickoff meeting with the Purchaser individually, and kickoff meeting with each additional Customer, and FL[DS] (if applicable) in accordance with the PO, and any applicable ATC.	The Contractor shall host the meeting within five (5) calendar days of PO issuance.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after deliverable due date.
2	The Contractor shall submit the Implementation Plan timely and in accordance with the PO and any applicable ATC.	The Contractor shall collaborate with the Customer and submit each Customer's Implementation Plan to the Purchaser and each additional Customer within 10 calendar days of PO issuance.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after the deliverable due date until the Customer Implementation Plan is received.  Financial consequences shall also be assessed for a Customer's Implementation Plan submitted that is not in accordance with the PO and any applicable ATC, in the amount of \$500 for each incomplete Implementation Plan.



**TABLE 1  
DELIVERABLES AND FINANCIAL CONSEQUENCES**

No.	Deliverable	Time Frame	Financial Consequences
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.
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.

<b>TABLE 1 DELIVERABLES AND FINANCIAL CONSEQUENCES</b>			
<b>No.</b>	<b>Deliverable</b>	<b>Time Frame</b>	<b>Financial Consequences</b>
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.
7	The Contractor shall report accurate information in accordance with the PO and any applicable ATC.	<p>QBRs are due 15 calendar days after the end of the quarter (January - March, April - June, July - September, and October - December).</p> <p>Monthly Implementation Reports are due five (5) calendar days after the end of the month.</p> <p>Monthly Training Reports are due five (5) calendar days after the end of the month.</p> <p>Monthly Service Reports are due five (5) calendar days after the end of the month.</p> <p>Ad hoc reports are due five (5) calendar days after the request by the Purchaser.</p>	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after any due date, until an accurate report is received.

**All deliverables are subject to the approval and acceptance of the Purchaser. Any deliverables rejected by the Purchaser will be subject to the applicable financial**

**consequences in Table 1 until the Contractor resubmits and the Purchaser accepts the deliverable.**

## **8.0 PERFORMANCE MEASURES**

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

### **8.1 Performance Compliance**

By submitting a response to this RFQ, the Contractor acknowledges and agrees that its performance under this SOW must meet the standards set forth above and that it will be bound by the conditions set forth herein. After executing an applicable financial consequence, the Purchaser may, at its sole discretion, allow additional time for the Contractor to remedy the performance issues identified by the Purchaser; or, after giving the Contractor a reasonable opportunity to cure such performance issues, may proceed with default proceedings.

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

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

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

## **9.0 FINANCIAL CONSEQUENCES**

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

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

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

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

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

**11.0 TIMELINE**

EVENT	DATE
Release of the RFQ	May 11, 2023
Pre-Quote Conference  Registration Link: <a href="https://us02web.zoom.us/join/https://us02web.zoom.us/meeting/register/tZllde6uqDkvG9QD2YQ4L4RJgTV_VFOdU23B">https://us02web.zoom.us/meeting/register/tZllde6uqDkvG9QD2YQ4L4RJgTV_VFOdU23B</a>	May 16, 2023, at 9:00 a.m., Eastern Time
Responses Due to the Procurement Officer, via email	May 22, 2023, by 5:00 p.m., Eastern Time
Solution Demonstrations and Quote Negotiations	May 23-25, 2023
Anticipated Award, via email	May 25, 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](mailto: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](mailto: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](mailto:PublicRecords@dms.fl.gov)**

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

**OTHER PURCHASER:**

**CONTRACT MANAGER SPECIFIED ON THE PO**

**20.3 Public Records Exemption**

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

**20.4 Document Management**

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

**21.0 IDENTIFICATION AND PROTECTION OF CONFIDENTIAL INFORMATION**

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

In the event of a request for public records pursuant to Chapter 119, F.S., the Florida Constitution, or other authority, to which records that are marked as "confidential" are responsive, the Agency will provide the vendor-redacted copy to the requestor. If a requestor asserts a right to the redacted Confidential Information, the Agency will notify the vendor



such an assertion has been made. It is the vendor's responsibility to take the appropriate legal action to assert that the information in question is exempt from disclosure under Chapter 119, F.S., or other applicable law.

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

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

## **22.0 USE OF SUBCONTRACTORS**

In providing services under the PO(s) and any applicable ATC, the Contractor is permitted to utilize subcontractors identified in its Quote. The Contractor shall notify the Contract Manager specified on the PO in writing of any subcontractors not identified in the Contractor's Quote who will be engaged to provide services for a PO 10 calendar days prior to their engagement. During the term of the PO, subcontractors may be substituted with the prior written approval of the Contract Manager specified on the PO. The Purchaser reserves the right to reject a subcontractor with 10 calendar days advance notification to the Contractor.

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

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

## **23.0 LEGISLATIVE APPROPRIATION**

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

## **24.0 MODIFICATIONS**

The Department reserves the right to change, add or delete any requirement from this RFQ if the Department deems it to be in the best interest of the State of Florida. In addition, the

Department reserves the right to withdraw and cancel this RFQ at any time, prior to a duly authorized and executed ATC or PO.

**25.0 CONFLICT OF INTEREST**

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

**26.0 DISCRIMINATORY, CONVICTED AND ANTITRUST VENDORS LISTS**

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

**27.0 E-VERIFY**

The Contractor (and its subcontractors) has an obligation to utilize the U.S. Department of Homeland Security's (DHS) E-Verify system for all newly hired employees in accordance with section 448.095, F.S. By accepting the ATC or any PO(s), the Contractor certifies that it is registered with, and uses, the E-Verify system for all newly hired employees in accordance with section 448.095, F.S. The Contractor must obtain an affidavit from its subcontractors in accordance with paragraph (2)(b) of section 448.095, F.S., and maintain a copy of such affidavit for the duration of any applicable ATC(s) and any PO(s). The Contractor shall provide a copy of its DHS Memorandum of Understanding (MOU) to the Contract Manager specified on the PO within five (5) business days of issuance of the ATC or any PO(s). The Contract Manager will be designated on any applicable ATC and PO.

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

**28.0 COOPERATION WITH INSPECTOR GENERAL**

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

**29.0 ACCESSIBILITY**

The Contractor will comply with section 508 of the Rehabilitation Act of 1973, as amended and 29 U.S.C. s. 794(d), including the regulations set forth under 36 C.F.R. part 1194. Section

282.601(1), F.S., states that “state government shall, when developing, competitively procuring, maintaining, or using electronic information or information technology acquired on or after July 1, 2006, ensure that State employees with disabilities have access to and are provided with information and data comparable to the access and use by State employees who are not individuals with disabilities.”

### **30.0 PRODUCTION AND INSPECTION**

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

### **31.0 SCRUTINIZED COMPANIES**

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

<https://www.sbafila.com/fsb/FundsWeManage/FRSPensionPlan/GlobalGovernanceMandate.s.aspx>.

### **32.0 BACKGROUND SCREENING**

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

#### **32.1 Background Check**

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

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

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

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

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

### **32.2 Disqualifying Offenses**

If at any time it is determined that a Person has a criminal misdemeanor or felony record regardless of adjudication (e.g., adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict) within the last six years from the date of the court’s determination for the crimes listed below, or their equivalent in any jurisdiction, the Contractor is required to immediately remove that Person from any position with access to State of Florida Data or directly performing services under the Contract. The disqualifying offenses are:

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

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

### **32.3 Refresh Screening**

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

### **32.4 Self-Disclosure**

The Contractor shall ensure that all Persons have a responsibility to self-report within three calendar days to the Contractor any updated court disposition regarding any

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

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

### **32.5 Duty to Provide Security Data**

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

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

### **32.6 Screening Compliance Audits and Security Inspections**

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

### **32.7 Record Retention**

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

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

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

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

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

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

### **32.8 Indemnification**

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

### **33.0 LOCATION OF DATA**

In accordance with Rule 60GG-4.002, F.A.C., the Contractor, including its employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees, or other persons operating under their direction, are prohibited from (i) performing any of the services under any applicable ATC or PO outside of the continental United States, or (ii)

sending, transmitting, storing, or accessing any State of Florida data, outside of the continental United States. The Parties agree that a violation of this provision will:

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

The credits or payments in subsection b) are a reasonable approximation of the internal costs for investigations and audits from a violation. The credits or payments are in the nature of liquidated damages and not intended to be a penalty. By executing any resulting ATC or performing under any resulting PO, the Contractor acknowledges and agrees the costs intended to be covered by subsection b) are not readily ascertainable and will be difficult to prove. The Contractor agrees that it will not argue, and is estopped from arguing, that such costs are a penalty or otherwise unenforceable. For purposes of determining the amount of costs due hereunder, a group of violations relating to a common set of operative facts (e.g., same location, same time period, same off-shore entity) shall be treated as a single violation. The costs will be applied as a financial consequence and are exclusive of any other right to damages.

### **34.0 DATA TRANSMISSION**

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

### **35.0 TERMS AND CONDITIONS**

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

**36.0 COOPERATIVE PURCHASING**

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

**37.0 PRICE ADJUSTMENTS**

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

**38.0 FINANCIAL STABILITY**

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

**39.0 RFQ ATTACHMENTS**

**Attachment A**, Price Sheet

**Attachment B**, Contact Information Sheet

Agency Term Contract (Redlines or modifications to the ATC are not permitted.)

Department's Purchase Order Terms and Conditions

Non-Disclosure Agreement (Redlines or modifications to the NDA are not permitted.)

**REMAINDER OF PAGE INTENTIONALLY LEFT BLANK**



## ATTACHMENT A PRICE SHEET

### I. Alternate Contract Source (ACS)

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

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

### II. Pricing Instructions

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

### III. Pricing

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



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

**V. Waterfall Pricing (Optional)**

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

**VI. State of Florida Enterprise Pricing (Optional)**

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

**VII. Value-Added Services (Optional)**

If vendors are able to offer additional services and/or commodities for a security operations platform 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**

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



FL [DIGITAL SERVICE]



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

## ReliaQuest Security Operations Platform Solution

**INCREASE VISIBILITY**

**REDUCE COMPLEXITY**

**REDUCE COSTS**

**MANAGE RISK**

## ATTACHMENT A PRICE SHEET

### I. Alternate Contract Source (ACS)

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

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

### II. Pricing Instructions

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

### III. Pricing

Initial Term Pricing (Years 1-3)		
Item No.	Description	Rate Per User
1	<p><b><u>Initial Software Year</u></b> One year of security operations platform software Solution as described in the RFQ per user. To include:</p> <ul style="list-style-type: none"> <li>• <b>implementation</b></li> <li>• <b>initial training</b></li> <li>• <b>initial Integration</b></li> <li>• integration maintenance</li> <li>• support services</li> </ul>	<p style="color: red;">See Attached ReliaQuest RFQ Response - Attachment A: Price Sheet</p> <p style="text-align: center;">\$ _____</p>
2	<p><b><u>Subsequent Software Year</u></b> One year of security operations platform software Solution as described in the RFQ per user. To include:</p> <ul style="list-style-type: none"> <li>• <b>ongoing training</b></li> <li>• integration maintenance</li> <li>• support services</li> </ul>	<p style="color: red;">See Attached ReliaQuest RFQ Response - Attachment A: Price Sheet</p> <p style="text-align: center;">\$ _____</p>

Optional Renewal Term Pricing (Years 4-6)		
Item No.	Description	Rate Per User
1	<p><b>Initial Software Year</b>                      One year of security operations platform software Solution as described in the RFQ per user. To include:</p> <ul style="list-style-type: none"> <li>• <b>implementation</b></li> <li>• <b>initial training</b></li> <li>• <b>initial Integration</b></li> <li>• integration maintenance</li> <li>• support services</li> </ul>	<p>See Attached ReliaQuest RFQ Response - Attachment A: Price Sheet</p> <p>\$ _____</p>
2	<p><b>Subsequent Software Year</b>                      One year of security operations platform software Solution as described in the RFQ per user. To include:</p> <ul style="list-style-type: none"> <li>• <b>ongoing training</b></li> <li>• integration maintenance</li> <li>• support services</li> </ul>	<p>See Attached ReliaQuest RFQ Response - Attachment A: Price Sheet</p> <p>\$ _____</p>

**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
	See Attached ReliaQuest RFQ Response - Attachment A: Price Sheet		

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	SKU Description	Market Price	ACS Price
	See Attached ReliaQuest		
	RFQ Response -		
	Attachment A: Price Sheet		

**V. Waterfall Pricing (Optional)**

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

**VI. State of Florida Enterprise Pricing (Optional)**

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

**VII. Value-Added Services (Optional)**

If vendors are able to offer additional services and/or commodities for a security operations platform 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.

Insight Public Sector  
 \_\_\_\_\_  
 Vendor Name

36-3949000  
 \_\_\_\_\_  
 FEIN

6/13/2023  
 \_\_\_\_\_  
 Date

*Lisanne Steinheiser*  
 \_\_\_\_\_  
 Signature

Lisanne Steinheiser  
 \_\_\_\_\_  
 Signatory Printed Name



**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**

	<b>Contact for Quoting Purposes</b>	<b>Contact for the ATC and PO (if awarded)</b>
<b>Name:</b>	Stephen Forsythe	Stephen Forsythe
<b>Title:</b>	Client Executive	Client Executive
<b>Address (Line 1):</b>	324 Cannonball Lane	324 Cannonball Lane
<b>Address (Line 2):</b>		
<b>City, State, Zip Code</b>	Watersound, FL 32461	Watersound, FL 32461
<b>Telephone (Office):</b>	501.505.4596	850-428-7966
<b>Telephone (Mobile):</b>		850-428-7966
<b>Email:</b>	TeamForsythe@Insight.com	Stephen.Forsythe@Insight.com



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  
INSIGHT PUBLIC SECTOR**

This Confidentiality and Non-Disclosure Agreement (“Agreement”) is between the Florida Department of Management Services (“Department”), a state agency, and Insight Public Sector (“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-22/23-157, Security Operations Platform 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**

**INSIGHT PUBLIC SECTOR**

By: \_\_\_\_\_

By: *Lisanne Steinheiser*

Name: \_\_\_\_\_

Name: Lisanne Steinheiser

Title: \_\_\_\_\_

Title: Global Compliance Officer

Date: \_\_\_\_\_

Date: 6/13/2023

FL [DIGITAL SERVICE]



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

---

## ReliaQuest Security Operations Platform Solution

**INCREASE VISIBILITY**

**REDUCE COMPLEXITY**

**REDUCE COSTS**

**MANAGE RISK**



## ReliaQuest - FL [DIGITAL SERVICE] & Respective State Agencies Executive Summary & Partnership Alignment

ReliaQuest has reviewed FL [DIGITAL SERVICE]'s RFQ for a Security Operations Platform Solution. Given the current partnership between the State of Florida and ReliaQuest, we feel we are uniquely positioned to expand our footprint and give the State better detection capability and visibility into the enterprise. Our ability to provide our platform at scale with custom capabilities matched to each State entity while being able to provide enterprise wide metrics on the health of the State puts us in

The ReliaQuest solution "GreyMatter" is a combination of both technology and blended service. The technology is a Security Platform based on an Open XDR architecture and delivered as a Service. The ReliaQuest solution is designed to increase visibility, eliminate complexity, and measurably manage and reduce cyber risk.

The ReliaQuest solution detailed below is tailored to the FL [DIGITAL SERVICE] and respective state agencies and uniquely aligned to support their initiatives around a unified SOC, and introduction of cost efficiencies via existing tool rationalization and consolidation.

The ReliaQuest solution provides FL [DIGITAL SERVICE] and respective state agencies with a fixed cost "all in" pricing model and eliminates much of the risk of additional and variable spend related to cyber security. Moreover, this solution will also be sized for complete visibility across the entire security ecosystem and be fully scalable to support future growth plans. As new additions or projects come forward, the ReliaQuest solution offers the speed and agility to secure these new ecosystem changes.

The ReliaQuest solution includes the optimization and management of new and/or existing SIEM platforms plus a full SOC offering designed to deliver greater automation and more complete value around the detection, investigation, and response process. Also included will be ReliaQuest's Digital Shadows Threat Intelligence solution. ReliaQuest will also assist with the optimization for greater realization of value gained by the various security tools FL [DIGITAL SERVICE] and respective state agencies own. This approach serves as a force multiplier for the existing team and improves the cost of ownership of current security tool spend.

The ReliaQuest solution is a "quick win" for FL [DIGITAL SERVICE] and respective state agencies. ReliaQuest can be fully operational in a matter of weeks following an initial Kick-off meeting within five (5) calendar days of PO issuance. ReliaQuest can also provide for an elegant migration from any existing provider and quickly snap-in to FL [DIGITAL SERVICE]'s and respective state agencies security ecosystem. Once in place, ReliaQuest's metrics and analytics begin delivering real time decision support allowing the program to immediately align to security frameworks, address gaps, and measurably improve and mature.

Below are key outcomes ReliaQuest will deliver on:

### Force Multiplier for Existing Team:

- Provide full incident investigations and response coverage with full transparency and coordination existing teams.
- Lessening the tuning burden on existing teams. ReliaQuest helps configure the proper detection coverage on FL [DIGITAL SERVICE] and respective state agency tools removing this arduous task from cyber security teams.
- Automation. Intelligent Analysis includes fully configured playbooks that automate the collection of key artifacts from various tools, enriched by threat intelligence and provides readily actionable research packages cutting response times to minutes not hours or days.
- Automated response initiates response actions across multiple tools on the fly and protects against a wide range of security threats including malware, phishing, insider threats, and zero-day attacks.
- Ability to collaborate with FL [DIGITAL SERVICE] and respective state agency SOC resources for effective investigations.

*How does ReliaQuest help?*

- GreyMatter Detect delivers signature and behavioral detection content configured for SIEM and EDR tools closing security gaps and best maximizing the value of these investments.
- GreyMatter API driven automation provides bi-directional integration to existing tools delivering automation and removes the complexity of having to pivot in and out of tools during the investigation process.





## Complement and Enhance Existing Investments

- Optimize existing FL [DIGITAL SERVICE] and respective state agency tools, including SIEM, EDR, perimeter solutions, email, cloud, etc. to fully maximize their capabilities.
- Metrics and Analytics to constantly provide feedback around team and tool efficacy and help IT teams rationalize tool spend.
- A platform and service that unifies existing technologies with transparency.
- Hands on support (health monitoring, configuration, upgrades, etc.)

### *How does ReliaQuest help?*

- ReliaQuest's GreyMatter SOC platform is based on an open XDR architecture, is fully vendor agnostic and integrates into the tools FL [DIGITAL SERVICE] and respective state agencies own today.
- ReliaQuest can fully support new and/or existing SIEM platforms as well as execute a plan to consolidate all agencies onto a common SIEM platform.
- ReliaQuest's Analytics engine tracks the alignment of existing tools to frameworks such as MITRE and NIST. This helps us deliver real time decision supporting metrics to close security gaps, increase tool efficacy and how best to protect the organization from new and emerging threats.

## Unified Visibility and Reduce Complexity

- Visibility across the entire FL [DIGITAL SERVICE] and respective state agency security ecosystem.
- Automated gathering of telemetry across existing in scope FL [DIGITAL SERVICE] and respective state agency security tool stack and business applications.
- Cut tool complexity from needing to pivot into, tune, and learn SIEM along with various other security controls.
- Visibility into 3<sup>rd</sup> party apps, multi-cloud, and disparate environments.
- Drive more efficiency, reduce complexity, and eliminate manual assessments.

### *How does ReliaQuest help?*

- ReliaQuest's customer success team will work with FL [DIGITAL SERVICE] and respective state agencies to ensure complete visibility into the various tools and applications regardless of location is achieved.
- ReliaQuest Intelligent Analysis removes the complexity of needing to navigate and learn multiple tool interfaces, pivot in and out different tools and manually work investigations. Via our Intelligence Analysis this is automated and worked by the ReliaQuest GreyMatter platform and services team.

---

## The Total Economic Impact™ of ReliaQuest

Recently, ReliaQuest commissioned a [Forrester® Total Economic Impact™ \(TEI\) study](#) to find out exactly what the financial and operational impact adopting the ReliaQuest offering can have on an organization.

Using Forrester's TEI methodology, the report found that the ROI of ReliaQuest is 350% over 3 years with a payback of less than 6 months, in addition to providing numerous other benefits, financial and otherwise.

Below are some of the most interesting findings on how ReliaQuest can positively impact a business in terms of cost, staffing, and overall security posture:

- **350% return on investment in three years**
- **< 6-month payback period**
- **20% increase in risk coverage**
- **\$440K reduction in legacy tools over three years**
- **\$1.2M avoidance in additional headcount**
- **A net-present value\* of \$5.51M**

## **GreyMatter Capabilities – What’s Included?**

Our collection of capabilities empowers FL [DIGITAL SERVICE] and respective state agencies along with ReliaQuest’s security teams to analyze and action threats from across your environment, from initial identification to running automated plays and monitoring ongoing health.

### **Intel – Threat Intelligence**

GreyMatter incorporates inputs from our security operations centers and over 40 other threat intelligence sources curated by our Digital Shadows Photon team to create a comprehensive view of existing and emerging threats that equips FL [DIGITAL SERVICE] and respective state agencies with the latest and most relevant threat intelligence. Intel is automatically prioritized and optimized for the FL [DIGITAL SERVICE] and respective state agencies environment, with continual tuning and validation ensuring relevant and actionable intelligence.

### **Detect – Use-Case Development / Tuning**

RQ provides full access to our extensive content library through a subscription model which allows immediate access to new content that is continually developed and/or updated by the ReliaQuest R&D team while we continuously tune your content to produce the highest fidelity alerts, to allow our teams as well FL [DIGITAL SERVICE] and respective state agencies to address critical events faster and more accurately.

### **Investigate**

GreyMatter will investigate all alerts to ensure FL [DIGITAL SERVICE] and respective state agencies are protected day and night. Our platform conducts advanced data aggregation and automations to accelerate threat analysis and containment to drive industry leading incident response in a fraction of the time, while enhancing the thoroughness of each investigation.

### **Hunt – Hunting Solution / Ongoing Hunt Campaigns**

GreyMatter provides the ability to schedule and execute focused threat hunting campaigns across disparate technologies within FL [DIGITAL SERVICE] and respective state agencies environments with the ability to aggregate and most importantly normalize data from multiple data sources, providing the most holistic view into an environment and the potential threats that may exist.

GreyMatter enables unlimited Hunt Campaigns that can be run by FL [DIGITAL SERVICE] and respective state agencies or scheduled by ReliaQuest.

### **Automate**

GreyMatter Integrates with key technologies across the enterprise to enrich, contain and/or remediate threats with fully configured playbooks to reduce the time and resources needed to mitigate threats or conduct investigations. GreyMatter Automate can integrate with existing ticketing systems to execute/build plays and allow RQ to drive tickets to remediation on approved actions.

### **Verify – Breach and Attack Simulation**

Automated and continuous cyber assurance and threat simulations provide accelerated recognition of security control failures and real-world insight into potential attack scenarios.

### **Health – SIEM Health and Performance Monitoring**

RQ conducts comprehensive, real-time monitoring of the health of your security environment through continual analysis of infrastructure, operating systems, applications, and integrations through sophisticated log source monitoring to actively baseline the environment and alert on deviations from normal activity.

## Analytics – Model Index

Operational and Board Level Analytics are designed to articulate risk, compare across industry and to guide our maturity roadmap for Visibility, Tool Efficacy and Team Performance.

## Ongoing Enablement

### Implementation

During Implementation, FL [DIGITAL SERVICE] and/or respective state agencies will go through a comprehensive onboarding process including workshops, health checks, log source verification, roadmaps, tabletop and direct engagement with engineering, threat management, and security analysts.

Implementation helps translate your business strategy into a set of measurable security program objectives while monitoring and measuring realized benefits to those outlined objectives.

Activities include:

- Review Current state, requirements, and expectations.
- Modeling of current environment & prioritization of business objectives
- Content and Health Check Workshop to build rulesets, communications plan and develop customer roadmap.
- Benefits Mapping for Executive Reporting & Dashboards
- Verification and Transition to Go-Live

## Customer Success Management

FL [DIGITAL SERVICE] and respective state agencies will be assigned a dedicated Customer Success Manager to be the single point of contact throughout the engagement. Your Customer Success Manager will ensure that ReliaQuest is providing the proposed services beyond expectations:

- Dedicated Customer Success Manager accountable for life cycle of FL [DIGITAL SERVICE] and respective state agencies ongoing success
- Proactive Communication - Daily communication providing in shift analyst contacts and end of shift summaries to ensure ticket handoff is seamless and no deterioration of results between shifts.
- Weekly call providing summary of any open tickets, status update on tools, content, processes, and progress along the RQ Maturity Roadmap
- Monthly communication and executive-ready reporting summarize results and recommendations.
- Quarterly executive reviews aligned to business goals, progression to roadmaps, adjustments, insights, gaps, accomplishments, and recommendations.
- Annual consolidated review, trending, comparison/benchmarking, roadmaps

## Business Analytics

Operational and Board Level Analytics designed to articulate risk, compare across industry and to guide our maturity roadmap for Visibility, Tool Efficacy and Team Performance – Helping our customers answer the following questions:

- How much of our environment can we see?
- Do we have the necessary detection controls in place?
- How well can we detect threats across the attack lifecycle?
- How well do we integrate threat intelligence into our program?
- Are we maximizing my tools capabilities?
- Is our tool's license optimized?
- How fast are we responding and resolving issues?
- How well does my team know our environment?
- How are we improving our False Positive Rate with precision tuning?



## SIEM Platform Engineering

ReliaQuest conducts comprehensive, real-time monitoring of the health of your security environment through continual analysis of infrastructure, operating systems, applications, and integrations through sophisticated log source monitoring. ReliaQuest supports the entire management / performance optimization of SIEM (log ingestion, performance, upgrades, capacity, etc.) to maximize performance but still allowing FL [DIGITAL SERVICE] and respective state agencies to retain administrative access.

## Detection Architecture and Engineering

Deliver Accelerated threat detection mapped to ATT&CK, MITRE, NIST, as well as other frameworks with continuous tuning to ensure fidelity alerting and increased visibility. Ongoing tuning and updates to all rules, dashboards and reports deployed – 24/7/365 tuning of alerts based on investigating findings and quarterly updates of all content based on Research & Development findings that align with FL [DIGITAL SERVICE] and respective state agencies threat landscape.

- Create security relevant use cases, documented, catalogued, and living in FL [DIGITAL SERVICE] and respective state agencies environments tied to business goals, risks and vulnerabilities with continuous tuning mapped to frameworks (NIST, MITRE, etc.) to baseline security coverage, prioritize areas of focus, and visualize progress.
- Threat intelligence and automation built into FL [DIGITAL SERVICE] and respective state agencies environments and on top of SIEM to improve speed of response and cost effectively scale security operation.

## Training

ReliaQuest will provide FL [DIGITAL SERVICE] and respective state agencies with ongoing training at no additional cost. Customers can have their employees go through training alongside ReliaQuest new employees or can set up one-off trainings directly with our training teams as needed.



### GreyMatter Service Level Agreement

ReliaQuest shall ensure that GreyMatter is Available for at least 99.9% of the time during each quarter of the term of an applicable order (the "Uptime SLA").

Unless otherwise agreed upon, services will not be performed outside of the continental United States and that State of Florida data will not be sent, transmitted, stored, or accessed outside of the continental United States in accordance with Section 33.0 of the RFQ and Rule 60GG-4.002, Florida Administrative Code.

### SLA Credits

If ReliaQuest fails to achieve the above Uptime SLA commitment for GreyMatter in any particular quarter during the term of an Order, Customer may claim a performance credit as shown below (the "SLA Credit").

PERCENTAGE AVAILABILITY PER CALENDAR QUARTER CREDIT	
99.9-100	NO CREDIT
99.0-99.9	1% of the Fee
95.0-99.0	2% of the Fee
0-95.0	5% of the Fee

### Exclusions

A Customer will not be entitled to an SLA Credit if it is in breach of its Agreement with GreyMatter, including payment obligations. No Uptime SLA commitment is provided for free, proof-of-concept or unpaid trial services of GreyMatter. In addition, the Uptime SLA commitment (and any associated SLA Credit) does not apply to any downtime, suspension or termination of GreyMatter that results from:

- Account suspension or termination due to Customer's breach of the terms of an Order.
- Routine scheduled maintenance performed by ReliaQuest or any unscheduled, emergency maintenance for an emergency caused by factors outside ReliaQuest's reasonable control.
- Force majeure events such as acts of God, acts of government, pandemic response, flood, fire, earthquake, civil unrest, and acts of terror.
- Other customer related issues, including but not limited to, any Customer alterations or changes to Customer's environment (including changes to customer IP addresses), Customer content or third-party content, or internet service provider failures or delays.
- Customer's equipment, software, any other technology used or relied upon by Customer, or any other third-party equipment, software or technology used by Customer or ReliaQuest that is required for access or use of GreyMatter, including any Third-Party Software or services.

### Service Credit Claims

To receive an SLA Credit, a Customer must file a claim for such SLA Credit within five (5) days following the end of the calendar quarter in which the Uptime SLA commitment was not met for GreyMatter, by notifying ReliaQuest in writing with a complete description of the downtime, how the Customer was adversely affected, and for how long. ReliaQuest reserves the right to deny the SLA Credit if the Customer does not qualify for such SLA Credit. The SLA Credit set forth in the Uptime SLA table above is the Customer's sole and exclusive remedy for the unavailability of GreyMatter.

### Definitions

"Availability" means that Customer is able to login to its GreyMatter account during the applicable calendar quarter, as determined by ReliaQuest.

"Customer" means the customer entity that is identified as a party to the Order, including any subsidiaries or affiliates.

"Fee" means twenty-five percent (25%) of the annual fee charged for GreyMatter as shown in the Order.

"GreyMatter" means the ReliaQuest GreyMatter software platform consisting of the GreyMatter Automate, GreyMatter Detect, GreyMatter Health, GreyMatter Hunt, GreyMatter Intel, GreyMatter Investigate, and GreyMatter Verify components, and any other related ReliaQuest software tools, programs, or platforms, whether existing now or developed by ReliaQuest during the term of an Order, including any enhancements, derivatives, or developments thereto.

"GreyMatter Automate" is the component of GreyMatter which supports the actions to enrich data and/or contain or remediate threats.

"GreyMatter Detect" is the component of GreyMatter which supports the overall content methodology and lifecycle to accelerate Customer's detection visibility and facilitate evolution of Customer's capabilities.

"GreyMatter Health" is the component of GreyMatter which supports the overall health of the primary technologies and is inclusive of all primary technologies.

"GreyMatter Hunt" is the component of GreyMatter which supports threat hunting potentially leveraging data from customer's primary and secondary technology.

"GreyMatter Intel" is the component of GreyMatter which supports threat intelligence automation, aggregation, normalization and dissemination of machine-readable threat intelligence.

"GreyMatter Investigate" is the component of GreyMatter which supports the triage and analysis of alerts which are generated within the customer's primary technology.



"GreyMatter Verify" is the component of GreyMatter which allows a Customer to test the effectiveness of Customer's cybersecurity tools and content by simulating malicious and/or anomalous activity in a benign manner, within Customer's environment.

"Order" means the applicable ordering document, statement of work, amendment, or other document used grant Customer access to GreyMatter.

"ReliaQuest" means ReliaQuest, LLC.

"Third-Party Software" means any software or software products made by a third party that are used by ReliaQuest, including but not limited to, ServiceNow, Thycotic, Amazon Web Services, Google Cloud Platform, elastic, and Azure.

### Ongoing Enablement – Service Level Agreement

This section outlines the associated service level agreements (“**OE SLAs**”) associated with Ongoing Enablement (as described in the Order). During the onboarding, the communication plan will be further defined however below are the outlined expected OE SLAs as part of this engagement.

The table below outlines the Measured SLAs for acknowledgement and analysis (either initial analysis or post analysis) by alert priority level. The acknowledgment Measured SLA timing will start when a RQ alert first appears in RQ Portal and is satisfied when the ticket is escalated or assigned to a RQ Resource and the RQ Portal status is modified to “In Progress”. The analysis Measured SLA timeframe begins once the ticket is moved to a “In Progress” status in RQ Portal and is satisfied when moved to a new status depending on investigation.

The OE SLAs will become enforceable three (3) months post implementation phase.

#### Incident Response SLAs for Investigate

Severity	Description	Acknowledgement/ Ticket Created	Initial/Post Analysis
<b>Critical</b>	Labeled RQ-SC-*	45 Minutes	60 Minutes
<b>High</b>	Labeled RQ-SH-*	60 Minutes	90 Minutes
<b>Medium</b>	Labeled RQ-SM-*	120 Minutes	240 Minutes
<b>Low</b>	Labeled RQ-SL-*	240 minutes	480 minutes

#### SLAs for SIEM Health Issues to be handled by Customer

During implementation ReliaQuest will work with customer to deploy custom ReliaQuest health content to assist in detecting log source issues. These alerts will be ticketed through the RQ Portal and automatically be sent to customers to action. ReliaQuest engineers will be available to assist customers with troubleshooting as needed.

#### Excused Non-Performance

ReliaQuest will not be responsible for the failure to meet any OE SLA for failure or inability to perform within the designated time frames or otherwise as a result of an occurrence on an issue outside of the control of ReliaQuest, including but are not limited to:

- VPN Connectivity Downtime
- Account Issues
- System Downtime Issues
- SMTP or Alert Forwarding Issues
- Failure to respond to tuning requests by RQ
- Other issues outside of RQ’s control

#### Definitions:

“EDR” means Endpoint detection and response.

“Measured SLA” means the acknowledgment and analysis (either initial analysis or post analysis) OE SLA’s for Incident Response SLAs for Investigate in each alert category by priority level (e.g. critical, high, medium and low), as measured on a monthly aggregate basis by taking the actual median response time during a month for each alert as determined by ReliaQuest (by category and priority) and comparing to targeted response time for such alert (by category and priority) as shown in the respective OE SLA table in this Addendum. Unless otherwise identified as a Measured SLA, any other OE SLAs contained in Addendum shall not be considered Measured SLAs for the purposes of this Addendum.

“Order” means the ordering document that this Addendum is attached to. “SIEM” means security, information, and event management

## Sample Implementation Plan







### Attachment A: Price Sheet

#### Notes:

- Pricing assumes that the procuring organization has at least a SIEM (Security Information & Event Management) solution or EDR (Endpoint Detection & Response) solution which is actively supported by GreyMatter or another solution that is supported by GreyMatter to receive alert telemetry
- Should a SIEM be required, ReliaQuest has provided GreyMatter SIEMaaS as an option for procuring entities. The proposed pricing are "Not to Exceed" numbers and can be revisited between the State of Florida, Insight and ReliaQuest as needed
- Under this RFQ and ACS, each Florida Enterprise Agency and State Customers are licensed for 3 GreyMatter Supported Technology Integrations. If additional integrations are desired, they can be purchased off the price book included in this RFQ and ACS
- Upon notice to ReliaQuest, the ReliaQuest Security Operations Platform can be transferred from the Purchaser to the Customer and back to the Purchaser if needed
- Implementation is included for all Enterprise Agencies
- Implementation is included for all Non-Enterprise Agencies

<b>GreyMatter License for State of Florida Non-Enterprise Agencies</b>			
<b>GreyMatter Licensed Entities</b>	<b>SKU</b>	<b>Description</b>	<b>Annual GreyMatter Enterprise License Cost</b>
0-50	GMENT-50	GreyMatter Enterprise license up to 50 State of Florida Non-Enterprise Agencies	\$4,484,348.60
50-100	GMENT-100	GreyMatter Enterprise license up to 100 State Florida Enterprise Non-Enterprise Agencies	\$4,612,748.60
100-200	GMENT-200	GreyMatter Enterprise license up to 200 State Florida Non-Enterprise Agencies	\$4,869,548.60
200-250	GMENT-250	GreyMatter Enterprise license up to 250 State Florida Non-Enterprise Agencies	\$6,527,000.00
250-300	GMENT-300	GreyMatter Enterprise license up to 300 State Florida Non-Enterprise Agencies	\$8,025,000.00
300-350	GMENT-350	GreyMatter Enterprise license up to 350 State Florida Non-Enterprise Agencies	\$9,148,500.00
350-400	GMENT-400	GreyMatter Enterprise license up to 400 State Florida Non-Enterprise Agencies	\$10,486,000.00
400-450	GMENT-450	GreyMatter Enterprise license up to 450 State Florida Non-Enterprise Agencies	\$11,877,000.00



450-500	GMENT-500	GreyMatter Enterprise license up to 500 State Florida Non-Enterprise Agencies	\$13,268,000.00
<b>GreyMatter Training Cost</b>			
<b>User Count</b>	<b>SKU</b>	<b>Description</b>	<b>Annual Price</b>
Unlimited	GMTrain-1	GreyMatter training per user	Included
<b>Annual GreyMatter Access Fee for State of Florida Non-Enterprise Agencies under CSOC Integration</b>			
<b>Employee Count</b>	<b>SKU</b>	<b>Description</b>	<b>Annual Price</b>
0-250	GMAccess-250	Annual Access Fee for State of Florida Non-Enterprise Agencies with up to 250 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$16,050.00
250 -750	GMAccess-750	Annual Access Fee for State of Florida Non-Enterprise Agencies with up to 750 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$26,750.00
750 -1500	GMAccess-1500	Annual Access Fee for State of Florida Non-Enterprise Agencies with up to 1500 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$40,125.00
1501 - 5000	GMAccess-5000	Annual Access Fee for State of Florida Non-Enterprise Agencies with up to 5000 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$64,200.00
5001 - 10000	GMAccess-10000	Annual Access Fee for State of Florida Non-Enterprise Agencies with up to 10000 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$96,300.00
10001 - 15000	GMAccess-15000	Annual Access Fee for State of Florida Non-Enterprise Agencies with up to 15000 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$133,750.00
<b>Annual GreyMatter Access Fee for State of Florida Non-Enterprise Agency with Enterprise License Threshold Met under CSOC Integration</b>			
<b>Employee Count</b>	<b>SKU</b>	<b>Description</b>	<b>Annual Price</b>
0-250	GMENTAcce ss-250	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to	\$96,300.00



		leverage the GreyMatter Enterprise Platform under the CSOC Integration	
250 -750	GMENTAccess-750	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$107,000.00
750 -1500	GMENTAccess-1500	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$120,375.00
1501 - 5000	GMENTAccess-5000	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$144,450.00
5001 - 10000	GMENTAccess-10000	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$176,550.00
10001 - 15000	GMENTAccess-15000	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform under the CSOC Integration	\$214,000.00
<b>GreyMatter License and Access Fee Not Under the CSOC Integration</b>			
<b>Employee Count</b>	<b>SKU</b>	<b>Description</b>	<b>Annual Price</b>
0-250	GMAccess-250	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform not under the CSOC Integration	\$149,800.00
250 -750	GMAccess-750	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform not under the CSOC Integration	\$160,500.00
750 -1500	GMAccess-1500	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform not under the CSOC Integration	\$173,875.00



1501 - 5000	GMAccess-5000	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform not under the CSOC Integration	\$197,950.00
5001 - 10000	GMAccess-10000	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform not under the CSOC Integration	\$230,050.00
10001 - 15000	GMAccess-15000	GreyMatter License and Access fee for a State of Florida Non-Enterprise Agency with up to 250 employees to leverage the GreyMatter Enterprise Platform not under the CSOC Integration	\$267,500.00

<b>Additional GreyMatter Supported Techonolgy Integration (Requires GreyMatter Access)</b>			
<b>Quantity</b>	<b>SKU</b>	<b>Description</b>	<b>Annual Price</b>
1	GMENTINT-1	GreyMatter supported technology integration directly into GreyMatter for data enrichment and automation for the State Customers and Enterprise Florida Agency under the CSOC Integration	\$254,660.00
1	GMINT-1	GreyMatter supported technology integration directly into GreyMatter for data enrichment and automation for a single State Customer instance of GreyMatter under the CSOC Integration	\$3,424.00
1	GMINT-2	GreyMatter supported technology integration directly into GreyMatter for data enrichment and automation for a single State Customer instance of GreyMatter not under the CSOC Integration	\$6,313.00
<b>Optional GreyMatter SIEMaaS (Requires GreyMatter Access)</b>			



EPS or GB/Day Equivalent	SKU	Description	Annual Price
1000	GMSIEMaaS-1000	GreyMatter SIEMaaS provided as part of the GreyMatter offering for a State Customer (in 1000 EPS increments or GB/Day equivalent)	\$16,145.23
<b>Optional GreyMatter Digital Risk Protection (Requires GreyMatter Access)</b>			
Entity	SKU	Description	Annual Price
1	RQDRP-250	GreyMatter Digital Risk Protection platform for a State Customer or Florida Enterprise Agency with up to 250 employees	\$20,865.00
1	RQDRP-750	GreyMatter Digital Risk Protection platform for a State Customer or Florida Enterprise Agency with up to 750 employees	\$27,713.00
1	RQDRP-1500	GreyMatter Digital Risk Protection platform for a State Customer or Florida Enterprise Agency with up to 1500 employees	\$35,288.60
1	RQDRP-5000	GreyMatter Digital Risk Protection platform for a State Customer or Florida Enterprise Agency with up to 5000 employees	\$49,850.23
1	RQDRP-10000	GreyMatter Digital Risk Protection platform for a State Customer or Florida Enterprise Agency with up to 10000 employees	\$56,100.10
1	RQDRP-15000	GreyMatter Digital Risk Protection platform for a State Customer or Florida Enterprise Agency with up to 15000 employees	\$65,794.30
<b>Optional GreyMatter Phishing Analyzer (Requires GreyMatter Access)</b>			
Entity	SKU	Description	Annual Price
0-250	GMPA-250	GreyMatter Phishing Analyzer for a State Customer or Florida Enterprise Agency with up to 250 employees	\$15,247.50
250 -750	GMPA-750	GreyMatter Phishing Analyzer for a State Customer or Florida Enterprise Agency with up to 750 employees	\$31,329.60
750 -1500	GMPA-1500	GreyMatter Phishing Analyzer for a State Customer or Florida Enterprise Agency with up to 1500 employees	\$44,586.90
1501 - 5000	GMPA-5000	GreyMatter Phishing Analyzer for a State Customer or Florida Enterprise Agency with up to 5000 employees	\$84,160.85



MAKE SECURITY POSSIBLE™

---

5001 - 10000	GMPA-10000	GreyMatter Phishing Analyzer for a State Customer or Florida Enterprise Agency with up to 10000 employees	\$99,991.50
10001 - 15000	GMPA-15000	GreyMatter Phishing Analyzer for a State Customer or Florida Enterprise Agency with up to 15000 employees	\$121,744.60

<b>Annual GreyMatter for State of Florida Enterprise Agency (select one of the options below)</b>			
<b>Quantity</b>	<b>SKU</b>	<b>Description</b>	<b>Price</b>
1	GMENT, GMTrain, GMAccess, GMSIEMaaS, and GMENTINT	GreyMatter License and Access fee for all State of Florida Enterprise Agencies to leverage the GreyMatter Enterprise Platform under the CSOC Integration to include GreyMatter training, 1 GreyMatter SIEMaaS integration for FL[DS], 20 GreyMatter integrations for data enrichment and automation for FL[DS], and managed services to operate the GreyMatter Enterprise Platform in the FL[DS] CSOC.	\$2,528,529.96 (Annual Advance Payment)
12	GMENT, GMTrain, GMAccess, GMSIEMaaS, and GMENTINT	GreyMatter License and Access fee for all State of Florida Enterprise Agencies to leverage the GreyMatter Enterprise Platform with CSOC Integration to include GreyMatter training, 1 GreyMatter SIEMaaS integration for FL[DS] annually, 20 GreyMatter integrations for data enrichment and automation for FL[DS] annually, and managed services to operate the GreyMatter Enterprise Platform in the FL[DS] CSOC.	\$215,688.33 (Monthly In Arrears)

# RELIAQUEST



CORPORATE RISK AND COMPLIANCE

Business Continuity and Disaster  
Recovery Plan

---



## Contents

Purpose and Overview .....	3
Plan Distribution .....	3
The Disaster Recovery Coordinator (DRC) .....	3
Disaster Management Team (DMT) .....	3
DMT General Responsibilities .....	4
The Disaster Recovery Team (DRT) .....	4
DRT General Responsibilities .....	4
Communication Plan .....	5
Internal to Staff .....	5
External to Customers .....	5
Employee Contact Details .....	5
Disaster Recovery Phases .....	5
Phase 1: Disaster Assessment .....	6
Phase 2: Disaster Recovery Activation .....	6
Phase 3: Alternate Site/Data Center Rebuild .....	6
Phase 4: Return to Normal Operations .....	6
Business Impact Analysis (BIA) .....	6
Recovery Time Objectives (RTO) .....	7
Recovery Point Objectives (RPO) .....	7
Primary Facilities & Emergency Contact Lists .....	7
Emergency Procedures .....	9
Plan Maintenance Schedule .....	9
Disaster Recovery Plan Testing .....	10
Disaster Recovery Team Training .....	10
Plan Revision History .....	12
Plan Approval .....	12
Appendix A: Suggested Responsibilities by Critical Functions .....	13
Appendix B: Sample Testing Documentation .....	14

## Purpose and Overview

ReliaQuest, LLC (the “Company” or “ReliaQuest”) will develop, implement, and maintain a Business Continuity and Disaster Recovery Plan (“BCDR” or “Plan”). The BCDR defines and documents business processes, applications, and assets critical to the business – processes that, if interrupted, would result in a material impact to business operations.

The primary focus of this document is to provide a plan to respond to a disaster that disrupts or significantly degrades one or more of ReliaQuest’s mission-critical functions. The intent is to be prepared to restore operations quickly and efficiently through reducing the number of decisions which must be made when, and if, a disaster occurs.

The Plan will be updated annually, when major changes occur, or when testing of all or a portion of the plan reveals a need. All plan changes must be made with approval of the designated Disaster Recovery Coordinator (DRC).

## Plan Distribution

The Plan will be available via the following methods:

- Electronically – Stored in a protected directory on the corporate file system, accessible on a need-to-know basis.
- Print Copy – A physical copy will be distributed to all members of the Disaster Management Team (DMT) annually or as needed.
- Employee Copies – All employees will receive Workday access to all need to know, emergency procedures, annexes, and appendixes.

## The Disaster Recovery Coordinator (DRC)

The function of the Disaster Recovery Coordinator (DRC) is essential to maintaining the readiness of each BCDR plan, annex, or appendix. The DRC assumes a lead position in the ongoing life and continuous improvement of the plan.

Primary responsibilities of the DRC:

- Distribution of the Disaster Recovery Plan
- Training the Disaster Recovery Teams
- Testing and rehearsal of the Disaster Recovery Plan
- Evaluating Disaster Recovery Plan Tests
- Updating Disaster Recovery Plan
- If Plan is activated, facilitating BCDR meetings and execution activities

## Disaster Management Team (DMT)

In the event an emergency or disaster occurs, the Disaster Management Team (DMT) will perform an initial assessment, confirm validity, understand general implications, and activate any applicable response plan as necessary. DMT members are listed below, authority

delegation and the ability to declare a disaster and activate the plan follows in chronological order of members.

<b>Name</b>	<b>Role</b>
Brian Murphy	Chief Executive Officer (CEO)
Colin O'Connor	Chief Operating Officer (COO)
Joe Partlow	Chief Technology Officer (CTO)
Greg Farrell	Chief Financial Officer (CFO)
John Burger	Chief Information Security Officer (CISO)
Regina Marrow	Chief Information Officer (CIO)
Brian Foster	Chief Product Officer
Jason Pfeiffer	Chief Strategy Officer
Mike McPherson	Sr. Vice President, Security Operations

### DMT General Responsibilities

- Provide strategic direction
- Assess an emergency and if necessary, declare a disaster and activate the applicable Plan
- Establish the structure of the Disaster Recovery Team (DRT) and supporting sub-elements
- Determine lead roles for functions that have been impacted by personnel loss
- Govern efforts of all recovery and operational teams
- Secure financial backing for the recovery effort
- Approve all actions that were not preplanned
- Expedite matters through all processes
- Provide guidance for media relations and external communications
- Define internal communications mechanisms
- Set periodicity of meetings and updates

### The Disaster Recovery Team (DRT)

In the event the DMT declares a disaster and activates the BCDR Plan, they may elect to establish a Disaster Recovery Team (DRT) upon which to delegate recovery roles and responsibilities. The Disaster Recovery Team (DRT) members will be comprised of, or appointed by members of the DMT and are responsible for coordination of assigned disaster recovery activities. If a DRT is established, all ReliaQuest recovery sub-teams, managers and supervisors will report to the DRT who will act as a liaison to the DMT.

### DRT General Responsibilities

- Assisting DMT assess extent and impact of damage
- Coordinating efforts of recovery activities as assigned by the DMT
- Monitoring and overseeing recovery activities of all recovery sub-teams
- Reporting recovery progress to the DMT
- Additional duties as assigned by DMT

Note: The CISO will be the Chair of the DRT and liaison to the DMT unless otherwise delegated.

In addition to general DRT responsibilities, Functional Support Teams (such as Financial, Technical and/or Logistics support) may be activated to provide specific recovery related functions. Please refer to Appendix A for brief outlines of suggested responsibilities by critical functions that may need to be activated during a disaster.

## Communication Plan

In the event of an emergency, instructions, and updates from the DMT will be disbursed via the following methods:

### Internal to Staff

- Corporate Yammer: <https://www.yammer.com/reliaquest.com/>
- Email Distribution List: [reliaquest@reliaquest.com](mailto:reliaquest@reliaquest.com)
- Microsoft Teams messages
- Preparis (Agility Recovery) - Mass Communication Platform
- Phone: 813.518.6565 or 800.925.2159
- Direct calls to employees
- Direct texts to employees

### External to Customers

- Email and/or phone call from customer's Customer Success Manager
- Messages in customer ServiceNow tickets
- Message on Company website: <http://www.reliaquest.com>
- Company Facebook page: <https://www.facebook.com/ReliaQuest>
- Company LinkedIn page <https://www.linkedin.com/company/240158>

### Employee Contact Details

Employees are responsible for ensuring their contact information (home address, mobile phone number, email, emergency contact, etc.) is accurate in Workday.

In the event of an emergency impacting a select department(s), affected department(s) managers will be contacted directly by a DMT appointee based on the specific type of emergency. If the department manager is unavailable for an extended period, an interim leader will serve as a temporary point of contact.

## Disaster Recovery Phases

The disaster recovery process consists of four phases:

- [Phase 1: Disaster Assessment](#)
- [Phase 2: Disaster Recovery Activation](#)
- [Phase 3: Alternate Site/Data Center Rebuild](#)
- [Phase 4: Return to Normal Operations](#)

### Phase 1: Disaster Assessment

The disaster assessment phase lasts from the inception of the disaster until the extent of the damage can be assessed. During this phase, cooperation with local, county and state officials, law enforcement, property management, and other designate partners is essential.

### Phase 2: Disaster Recovery Activation

This phase begins if the decision is made to move primary processing to another location. The DMT will assemble, may create specialized functional support teams, and call upon individual team members to perform required response tasks. The most important function is to fully restore operations at a suitable location and resume normal operations. Once normal operations are established at the alternate location, Phase 2 is complete.

### Phase 3: Alternate Site/Data Center Rebuild

Phase involves continuing operations at the alternate location while simultaneously undertaking the process of restoring the primary site and/or data center.

### Phase 4: Return to Normal Operations

Phase involves reactivation of primary site at either original or potentially a new location. At the end of this phase, a thorough review of the disaster recovery process should be taken. Any identified deficiencies during the utilization of the Plan will be reported to and corrected by the DRC.

## Business Impact Analysis (BIA)

Not all business activities can be immediately continued following a disaster. ReliaQuest must determine functions required for continuity of business functions. Disaster Recovery is the phased restoration of mission-critical services, functions, and operations.

A Business Impact Analysis (BIA) is periodically performed to determine which tasks and functions are critical for ReliaQuest to sustain business.

This recovery of each task or function is then associated with specific timeframes and criticalities to the business.

- Mission Critical (“Critical”): ***Urgent restoration is required as the business can no longer deliver*** on Service Level Agreements, contracted requirements or critical business functions resulting in work stoppage. Mission Fails.
- Mission Essential (“High”): ***Immediate restoration is required*** as our ability to deliver on Service Level Agreements, contracted requirements or critical business functions is ***severely degraded*** with no reasonable workaround. Mission is Severely Degraded.
- Mission Impacting (“Medium”): ***Restoration is required*** as our ability to deliver on Service Level Agreements, contracted requirements or critical business functions is ***somewhat degraded***. Acceptable workarounds are available, but do not provide the same level of effectiveness. Mission is Degraded.
- Non-Impacting (“Low”): ***Restoration can be deferred*** as business functions can continue but not at the same level of efficiency. Mission is less efficient.

In advance of a disaster or emergency, ReliaQuest will enumerate each applicable device, service, and application and assign it a recovery criticality of Critical, High, Medium, or Low based on above criteria.

## Recovery Time Objectives (RTO)

The Recovery Time Objectives (RTO) reflect the estimated recovery times based on current configurations and operations. They are the maximum amount of time allowed to resume an activity, recover resources, or provide products and services after a disruptive incident occurs. The target time periods must be reviewed periodically to ensure they are short enough that adverse impacts do not become unacceptable and are attainable.

RTO Thresholds	Recovery Goal
Mission Critical (“Critical”)	2 hours
Mission Essential (“High”)	8 hours
Mission Impacting (“Medium”)	Set by Resource Owner or CISO
Non-Impacting (“Low”)	Set by Resource Owner or CISO

## Recovery Point Objectives (RPO)

Recovery Point Objective (RPO) refers to a data recovery objective that must be achieved to allow an activity to resume after a disruptive incident has occurred. It reflects the estimated point in time to which recovery would be made based on current configurations and operations. The exact recovery point for each server, system, or application will vary due to the specific time when the most recent backup took place and when the disaster occurs.

Hardware, Service or Software PRO	Recovery Goal
Mission Critical (“Critical”)	2 hours
Mission Essential (“High”)	8 hours
Mission Impacting (“Medium”)	Set by Resource Owner or CISO
Non-Impacting (“Low”)	Set by Resource Owner or CISO

## Primary Facilities & Emergency Contact Lists

Name	Address	Facility Purpose	Main Phone Number	Facility Management Company & Contact Info
ReliaQuest Tampa Water Street	1001 Water Street, Suite 1900 Tampa, FL 33602	Corporate Headquarters & SOC	813.675.1010	Cushman Wakefield  Lizbeth Strother, Sr. Assist. Property Mgr Direct: 813.465.7014 Cell: 813.455.4179 lizbeth.strother@cushwake.com  Chris Brown, General Manager Direct: 813.204.5303

				Mobile: 813.924.6413 chris.d.brown@cushwake.com
ReliaQuest Tampa Harbour Island	777 South Harbor Island, Suite 500 Tampa, FL 33602	SOC	813.518.6565	Highwoods  Georgina Manragh, Property Manager Office 813.222.8834 Mobile 813.781.7314 Georgina.Manragh@highwoods.com
Flexential Data Center	8350 Parkedge Dr, Tampa, FL 33637	Colocation center	866.351.0670	Flexential  866.351.0670
ReliaQuest Las Vegas	7450 Arroyo Crossing Pkwy, Suite 100 Las Vegas, NV 89113	SOC & corporate operations	813.675.1010	EJM Development  Billie Jean Sclafani, Nevada Portfolio Manager Office: 702.597.1852 Cell: 702.400.5041 bsclafani@ejmdevelopment.com
Switch Data Center	5057-5199 W Warm Springs Rd Las Vegas, NV 89118	Colocation center	877.360.6283	Switch  877.360.6283
ReliaQuest Dublin	Cairn House, South County Business Park, 2nd Floor, Leopardstown, Dublin 18, Ireland	SOC & corporate operations	813.675.1010	Aramark Property  Ciaran Curley, Associate Director Direct: +353.1.871.5400 Mobile: +353.87.776.2723 curley-ciaran@aramark.ie
ReliaQuest SLC	9785 Monroe Street, Suite 102 Sandy, UT 84070	Innovation & corporate operations	813.675.1010	Woodbury Corporation LJ Heaton lj_heaton@woodburycorp.com 801.209.2167
ReliaQuest India	2nd Floor, UrbanWrk Private Limited, Westport Building, Pan Card Club Rd, Baner, Pune, Maharashtra 411045, India	Innovation & SOC	813.675.1010	UrbanWrk <a href="https://urbanwrk.in/">https://urbanwrk.in/</a> +91 70835 19892
ReliaQuest London	Columbus Building, Level 6, 7	Corporate operations	813.675.1010	Canary Wharf Group

	Westferry Circus, London E14 4HD, United Kingdom		Adam Robinson, Building Manager <a href="mailto:Adam.robinson@canarywharf.com">Adam.robinson@canarywharf.com</a>  Pamela Dunkley, Building Security <a href="mailto:B2security@canarywharf.com">B2security@canarywharf.com</a> +442074182809
--	--	--	---

## Emergency Procedures

- Facility Evacuation (Annex A)
- Fire Emergency (Annex B)
- Computer Incident (Annex C)
- Pandemic (Annex D)
- Physical Security Threats
- Bomb Threat (Annex E)
- Suspicious Package (Annex F)
- Hurricane (Annex G)
- ReliaQuest Facility Loss
- Tampa Headquarters Facility Loss (Annex H)
- Las Vegas Facility Loss (Annex I)
- Dublin, Ireland Facility Loss (Annex J)
- Data Center Failover (Annex K)
- Las Vegas Data Center Loss (Annex L)

## Plan Maintenance Schedule

Period	Action
Quarterly	Review all personnel and role changes and update plan accordingly
Quarterly	Have any new software, applications, or service offerings been implemented? If so, have all disaster recovery implications been addressed?
Quarterly	Any major changes to existing software, applications, or services? If so, update the recovery plan accordingly
Quarterly	Has the hardware configuration changed? If the changes affect our ability to recover, make appropriate changes to the recovery configuration.
Quarterly	Update the Network Configuration Diagrams
Quarterly	Verify off-site DR location availability and ensure suitability
Quarterly	Ensure all team assignments are still valid
Quarterly	Ensure all contact lists are current
Annually	Test a plan procedure and update it based on the results of the test
Annually	Review backup image retention requirements



Annually	Review insurance coverage
Annually	Update Plan in its entirety

## Disaster Recovery Plan Testing

The Disaster Recovery Coordinator (DRC) is accountable for updating the disaster recovery plan in its entirety, annually and testing a plan procedure annually. Whenever there has been a major revision to the plan or significant changes in the environment, the plan will be tested, regardless of any previous testing.

Note: If a portion of the Plan is activated and properly documented, this will qualify as a test of the Plan for the given period.

The objectives of testing the disaster recovery plan are as follows:

- Simulate the conditions of an actual recovery situation
- Determine feasibility of the recovery process
- Identify deficiencies in existing procedures
- Test completeness of business recovery information and alternate facility suitability
- Train members of the disaster recovery teams
- Optimize and update the plan for continuous improvement maturity

The initial test of the plan procedure will be in the form of a structured walk-through and should occur within two months of the plan procedure's acceptance. Subsequent scheduling of tests shall be determined based on the degree of readiness, relative costs and time to exercise a given plan. Refer to Appendix C for a sample recovery test agenda template.

## Disaster Recovery Team Training

The Disaster Recovery Coordinator is accountable for coordination of training relating to the disaster recovery plan. The purpose of this training is twofold:

- To train recovery team participants who are required to execute plan segments in the event of a disaster.
- To train ReliaQuest management and key employees in disaster prevention and awareness and the need for disaster recovery planning.

A Disaster Recovery Plan must have continued support from ReliaQuest's management to ensure future effective participation in plan testing and updating. It is not solely the responsibility of the Disaster Recovery Coordinator to suggest updates to the disaster recovery plan.

Management must be aware of the basic recovery strategy; how the plan provides for rapid recovery of their information technology systems support structure; and how plans effectiveness may be compromised as business operations evolve and expand significantly without notification to the Disaster Recovery Coordinator.

It is the responsibility of each recovery team participant to fully read and comprehend the entire plan, with specific emphasis on their role and responsibilities as part of the recovery team. On-going training of the recovery team participants will continue through plan tests and review of the plan contents and updates provided by the Disaster Recovery Coordinator.

Refer to Appendix D for a sample recovery training log template.

## Plan Revision History

Contributor	Date	Version	Changes
Joe Partlow	6/7/2013	1.0	Initial Document
Joe Partlow	5/14/15	1.5	Minor revisions for SOC 2
Joe Partlow	10/1/15	2.0	Staff and redundant SOC Changes
Nick Jackson	1/6/2015	2.1	Minor changes to Backup and Recovery
Joe Partlow	2/11/2016	2.2	Updated failover office
Joe Partlow	2/26/2016	2.3	Minor wording edits
Joe Partlow	10/4/2016	2.4	Staffing updates & staff failover plan
Chris Martinez	06/09/2017	2.5	Updated locations
John Burger	03/09/2018	2.6	Annual Review
Travis Kober	02/08/19	2.7	Updated formatting, verbiage and inclusion of Ireland Facility
Travis Kober	12/06/2019	2.8	Added SLC Technology Center facility details
Travis Kober	3/02/20	2.9	Annual review
John Burger	2/6/2021	3.0	Annual review and approval
Shazia Saeed	3/22/2022	3.1	Annual review and updates
John Burger	4/2/2022	3.1	Annual review and approval
Regina Marrow	4/11/2023	3.2	Annual review and approval

## Approved by

*Regina Marrow*

Regina Marrow  
Chief Information Officer  
April 11, 2023

## Appendix A: Suggested Responsibilities by Critical Functions

### **Administrative, Personnel, and Financial Support Team**

The administrative and financial team responsibilities include:

- Hiring temporary help and reassigning personnel as appropriate
- Expediting necessary purchase requests and accounting for recovery costs
- Notifying all vendors and delivery services of change of address for new facilities as appropriate
- Handling all personnel matters

### **Technical Support Team**

The Technical function responsibilities include:

- Coordinating acquisition, configuration, installation, and restoration of technical capabilities
- Securing correct backups for restoration
- Bringing up systems and restoring from data backups
- Maintaining systems software at the alternate site
- Providing technical support to teams
- Providing/restoring voice and data communications at the primary and alternate sites

### **Facility and Logistics Support Team**

The Facility and Logistics Support Team responsibilities include:

- Developing the fit-up plan for temporary facilities
- Working with Procurement to expedite the purchase required logistics, transportation and supplies
- Executing or outsourcing execution of facilities fit-up
- Minimizing damage at the primary site and working with the insurance company for expedient settlement of all claims. This is dependent

## Appendix B: Sample Testing Documentation

### Sample Recovery Test Agenda

1. What is the PURPOSE of the test?
2. What are the test OBJECTIVES?
3. How will the successful achievement of these objectives be measured?
4. At the end of the test, collect test measurements/feedback from all participants.
5. Evaluate test results. Determine if the test was successful or not (where the objectives met?).
6. Determine the implications of test results. Does success for this test imply success in all recovery scenarios?
7. Update plan based on results of the test.

### Sample Recovery Test History Form

Date	Type	Objective	Results

### Sample Recovery Test Plan

Test Date \_\_\_\_\_ Test # \_\_\_\_\_

Test Objectives:

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_

Task Number	Task Description	Completed (X)
-------------	------------------	---------------

T010	Determine appropriate test date	T010
T020	Schedule a test date	T020
T030	Meet and plan preliminary test criteria and goals	T030
T040	Determine who will be participating in the test	T040
T050	Meet with entire test team to discuss goals and objectives	T050
T060	Determine hardware requirements	T060
T070	Determine software requirements	T070
T080	Determine printing requirements	T080
T090	Determine network requirements.	T090
T100	Determine what images need to be used for the test	T100
T110	Determine what other documentation needs to be brought to the test location	T110
T120	Determine if blank medium components are needed for test and plan accordingly	T120
T130	If necessary, call vendors with licensing dependent products and get required information to run products on the test systems	T130
T140	Get network specific information	T140
T150	Final meeting to review plans	T150
T160	Pack backups and other supplies for test	T160
T170	Perform test following procedures in the test script	T170
T180	Conduct post-test debriefing before leaving test site	T180
T190	Remove data from test system disk drives	T190
T200	Destroy confidential information	T200
T210	Pack backups for return home	T210
T220	Gather documentation from all test teams	T220
T230	Complete documenting the test	T230
T240	Meet with test participants and analyze the test	T240
T250	Update disaster recovery manual based on test results	T250

## Sample Test Evaluation Form

### BCDR Test Report

**BCP Name:** Click or tap here to enter text.

**Business Area:** Click or tap here to enter text.

**BCP Test Lead:** Click or tap here to enter text.

**Test Type:** Choose an item.

**Test Date:**

**Participants:**

**Describe the test scenario used:**

**Describe the aspects that worked well during the test:**

**Were the test objectives met?**

**Describe lessons learned, areas identified for improvement and follow up action items:**

**Recommended actions**

**Assignee**

**Completion Date**

.....

.....

.....

.....

.....






# Insight Response - ReliaQuest 61323 Completed

Final Audit Report

2023-06-13

Created:	2023-06-13
By:	AMANDA LUEDY (AMANDA.LUEDY@INSIGHT.COM)
Status:	Signed
Transaction ID:	CBJCHBCAABAAAs8A1IGdEXo8rl7M7tw3MJkD-bXnIQUAu

## "Insight Response - ReliaQuest 61323 Completed" History

-  Document created by AMANDA LUEDY (AMANDA.LUEDY@INSIGHT.COM)  
2023-06-13 - 5:45:48 PM GMT- IP address: 198.187.200.254
-  Document emailed to Lisanne Steinheiser (lisanne.steinheiser@insight.com) for signature  
2023-06-13 - 5:47:22 PM GMT
-  Email viewed by Lisanne Steinheiser (lisanne.steinheiser@insight.com)  
2023-06-13 - 5:47:46 PM GMT- IP address: 104.47.58.254
-  Document e-signed by Lisanne Steinheiser (lisanne.steinheiser@insight.com)  
Signature Date: 2023-06-13 - 5:47:56 PM GMT - Time Source: server- IP address: 20.125.67.140
-  Agreement completed.  
2023-06-13 - 5:47:56 PM GMT



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

**Section 1. Purchase Order.**

**A. Composition and Priority.**

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

**B. Initial Term.**

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

**Section 2. Performance.**

**A. Performance Standards.**

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

**B. Performance Deficiency.**

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

**Section 3. Payment and Fees.**

**A. Payment Invoicing.**

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

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

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

**B. Payment Timeframe.**

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

**C. MyFloridaMarketPlace Fees.**

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

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

**D. Payment Audit.**

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

**E. Annual Appropriation and Travel.**

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

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

**Section 4. Liability.**

**A. Indemnity.**

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

**B. Payment for Claims.**

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

**C. Liability Insurance.**

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

**D. Workers' Compensation.**

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

**E. Performance Bond.**

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

**Section 5. Compliance with Laws.**

**A. Conduct of Business.**

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

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

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

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

**B. Lobbying.**

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

**C. Gratuities.**

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

**D. Cooperation with Inspector General.**

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

**E. Public Records.**

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

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

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

**F. Communications and Confidentiality.**

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

**G. Intellectual Property.**

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

**H. Convicted and Discriminatory Vendor Lists.**

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

**Section 6. Termination.**

**A. Termination for Convenience.**

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

**B. Termination for Cause.**

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

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

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

**Section 7. Subcontractors and Assignments.**

**A. Subcontractors.**

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

**B. Assignment.**

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

**Section 8. RESPECT and PRIDE.**

**A. RESPECT.**

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

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

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

**B. PRIDE.**

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

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

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

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

**Section 9. Miscellaneous.**

**A. Independent Contractor.**

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

**B. Governing Law and Venue.**

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

**C. Waiver.**

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

**D. Modification and Severability.**

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

**E. Time is of the Essence.**

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

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

**F. Background Check.**

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

**G. E-Verify.**

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

**H. Commodities Logistics.**

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

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

**REMAINDER OF PAGE INTENTIONALLY LEFT BLANK**





4050 Esplanade Way  
Tallahassee, FL 32399-0950

**Ron DeSantis, Governor**  
Pedro Allende, Secretary

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

This Confidentiality and Non-Disclosure Agreement (“Agreement”) is between the Florida Department of Management Services (“Department”), a state agency, and Insight Public Sector (“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-22/23-157, Security Operations Platform 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**

**INSIGHT PUBLIC SECTOR**

DocuSigned by:  
By: *Pedro Allende*  
5E91A9D369EB47C...

By: *Stephen Forsythe*

Name: Pedro Allende

Name: Stephen Forsythe

Title: Secretary

Title: Client Executive

Date: 6/14/2023 | 5:01 PM EDT

Date: 5/23/23