

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

---

**AGENCY TERM CONTRACT  
FOR  
ENDPOINT DETECTION AND RESPONSE  
DMS-22/23-155E  
BETWEEN  
STATE OF FLORIDA  
DEPARTMENT OF MANAGEMENT SERVICES  
AND  
PC SOLUTIONS AND INTEGRATION**

## 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 PCS. (Contractor), with offices at 4937 SW 75<sup>th</sup> Avenue, Miami, FL 323155, each a “Party” and collectively referred to herein as the “Parties”.

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

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

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

### 1.0 Definitions

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

### 2.0 Scope of Work

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

### 3.0 Contract Term

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

### 4.0 Renewal Terms

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

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

## 5.0 Contract Documents and Hierarchy

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

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

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

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

## 6.0 Amendments

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

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

## 7.0 Contract Notices

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

## 8.0 Contract Contacts

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

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

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

David Rudnick  
VP of Sales  
4937 SW 75th Avenue  
Miami, FL 33155  
Telephone: (786) 391-4748  
Email: [david@pcsusa.net](mailto:david@pcsusa.net)

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

## **9.0 Assignment**

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

## **10.0 Price Decreases**

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

## **11.0 Additions/Deletions**

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

## **12.0 Cooperative Purchasing**

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

## **13.0 Other Conditions**

### **13.1 Independent Contractor Status**

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

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

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

**13.2 Force Majeure**

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

**13.3 Cooperation with the Florida Senate and Florida House of Representatives**

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

**13.4 Employment of State Workers**

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

**SIGNATURE PAGE IMMEDIATELY FOLLOWS**

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

PC SOLUTIONS AND INTEGRATION:

STATE OF FLORIDA  
DEPARTMENT OF MANAGEMENT SERVICES:

DocuSigned by:  
*Rob Boush*  
C6EF9A20D2BA436...  
Authorized Signature

DocuSigned by:  
*Pedro Allende*  
5E91A9D369EB47C...  
Pedro Allende, Secretary

Rob Boush  
Print Name

6/29/2023 | 3:33 PM EDT  
Date

Account Manager  
Title

6/29/2023 | 11:52 AM EDT  
Date

## Exhibit "A"

### Request for Quotes (RFQ)

#### DMS-22/23-155

### Endpoint Detection and Response Solution

#### Alternate Contract Sources:

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

#### 1.0 **DEFINITIONS**

The following definitions shall apply throughout this RFQ:

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

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

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

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

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

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

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

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



## **2.0 OBJECTIVE**

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

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

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

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

## **3.0 DESCRIPTION OF PURCHASE**

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

## **4.0 BACKGROUND INFORMATION**

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

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

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

## 5.0 **TERM**

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

## 6.0 **SCOPE OF WORK**

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

### 6.1. **Software Solution/Specifications**

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

#### 6.1.1. Multi-Tenant

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

#### 6.1.2. Scalability

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

### **6.1.3. Cloud Management**

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

### **6.1.4. Managed Security Services**

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

### **6.1.5. Prevention**

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

### **6.1.6. Product Usability**

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

### **6.1.7. Administration and Management Usability**

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

### **6.1.8. Endpoint Detection and Response**

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

### **6.1.9. Endpoint Protection Platform Suite**

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

### **6.1.10. Operating System Support**

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

#### **6.1.11. Data Management and Storage**

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

#### **6.1.12. Performance Management**

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

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

#### **6.1.13. Security**

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

#### **6.1.14. Data Management**

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

#### **6.1.15. Disaster Recovery and Backup**

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

#### **6.1.16. Identity and Access Management**

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

#### **6.1.17. Network**

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

#### **6.1.18. Compliance and Third-Party Certification**

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

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

#### **6.1.19. Configuration and Customization**

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

#### **6.1.20. Role-Based Access**

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

#### **6.1.21. Data Export**

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

#### **6.1.22. Integration**

- 6.1.22.1.** The Solution shall integrate with the Department's existing security tools such as firewalls, antivirus software, endpoint management solutions and security information and event management (SIEM) systems. The Customer shall determine if the Solution is able to integrate with the Customer's security tools. The Contractor shall take any steps necessary to support Customer integration.
- 6.1.22.2.** The Solution shall be capable of data integration through common exchange techniques and frameworks such as RESTful Application Programming Interfaces (APIs).
- 6.1.22.3.** The Solution shall be capable of integrating with a variety of identity and access management (IAM) systems to meet Customer current and future needs.
- 6.1.22.4.** Initial Integration shall include connecting each Customer to the state Cybersecurity Operations Center (CSOC) and validating with FL[DS] that all Solution data is properly integrated, as requested by the Customer.
- 6.1.22.5.** Integration Maintenance may be required after initial integration to ensure that the Solution properly exchanges data between Customers and the CSOC. The Contractor shall address any concerns that FL[DS] has regarding integration issues.

### **6.1.23. Performance and Availability**

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

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

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

### **6.2. Training and Support**

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

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

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

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

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

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

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

### **6.3. Kickoff Meeting**

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

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

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

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

#### 6.4. **Implementation**

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

The Implementation Plan must include the following at a minimum:

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

#### 6.5. **Reporting**

The Contractor shall provide the following reports to the Purchaser:

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

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

## 6.6. Optional Services

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

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

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

### 6.6.2. Future Integrations

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

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

## 7.0 DELIVERABLES

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



**TABLE 1  
DELIVERABLES AND FINANCIAL CONSEQUENCES**

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

**TABLE 1  
DELIVERABLES AND FINANCIAL CONSEQUENCES**

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

**TABLE 1  
DELIVERABLES AND FINANCIAL CONSEQUENCES**

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

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

## **8.0 PERFORMANCE MEASURES**

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

### **8.1 Performance Compliance**

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

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

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

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

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

## **9.0 FINANCIAL CONSEQUENCES**

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

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

## **10.0 RESPONSE CONTENT AND FORMAT**

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

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

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

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

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

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

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

## 11.0 **TIMELINE**

EVENT	DATE
Release of the RFQ	May 10, 2023
Pre-Quote Conference  Registration Link: <a href="https://us02web.zoom.us/j/8442675035">https://us02web.zoom.us/j/8442675035</a>	May 15, 2023, at 2:00 p.m., Eastern Time
Responses Due to the Procurement Officer, via email	May 19, 2023, by 5:00 p.m., Eastern Time
Solution Demonstrations and Quote Negotiations	May 22-24, 2023
Anticipated Award, via email	May 24, 2023

**12.0 PROCUREMENT OFFICER**

The Procurement Officer for this RFQ is:

Alisha Morgan  
Department of Management Services  
4050 Esplanade Way  
Tallahassee, FL 32399-0950  
[DMS.Purchasing@dms.fl.gov](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.sbafla.com/fsb/FundsWeManage/FRSPensionPlan/GlobalGovernanceMandates.aspx>.

### **32.0 BACKGROUND SCREENING**

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

#### **32.1 Background Check**

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

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

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

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

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

#### **32.2 Disqualifying Offenses**

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

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

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

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

### **32.3 Refresh Screening**

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

### **32.4 Self-Disclosure**

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

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

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

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

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

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

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

### **32.7 Record Retention**

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

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

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

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

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

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

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

### **32.8 Indemnification**

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

### **33.0 LOCATION OF DATA**

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

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

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

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

**34.0 DATA TRANSMISSION**

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

**35.0 TERMS AND CONDITIONS**

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

**36.0 COOPERATIVE PURCHASING**

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

**37.0 PRICE ADJUSTMENTS**

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

**38.0 FINANCIAL STABILITY**

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

**39.0 RFQ ATTACHMENTS**

**Attachment A**, Price Sheet  
**Attachment B**, Contact Information Sheet



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

**REMAINDER OF PAGE INTENTIONALLY LEFT BLANK**

## ATTACHMENT A PRICE SHEET

### I. Alternate Contract Source (ACS)

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

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

### II. Pricing Instructions

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

### III. Pricing

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

Optional Renewal Term Pricing (Years 4-6)		
Item No.	Description	Rate Per Device
1	<p><b>Initial Software Year</b>                      One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> <li>• implementation</li> <li>• initial training</li> <li>• initial Integration</li> <li>• integration maintenance</li> <li>• support services</li> </ul>	\$ _____
2	<p><b>Subsequent Software Year</b>                      One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> <li>• ongoing training</li> <li>• integration maintenance</li> <li>• support services</li> </ul>	\$ _____

**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

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

**V. Waterfall Pricing (Optional)**

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

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

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

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

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

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

\_\_\_\_\_  
Vendor Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
FEIN

\_\_\_\_\_  
Signatory Printed Name

\_\_\_\_\_  
Date

**ATTACHMENT B  
CONTACT INFORMATION SHEET**

---

**I. Contact Instructions**

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

**II. Contact Information**

	<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>		

**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**



**PREPARED FOR:** Department of Management Services, State of Florida  
Response to RFQ #: DMS-22/23-155 - Endpoint Detection and  
Response Solution

PC Solutions & Integration, Inc.  
Simplify with Technology

**CREATED:** May 15th, 2023

PREPARED BY: Vishal Nanda

**W:** [www.pcsusa.net](http://www.pcsusa.net)

**E:** [vnanda@pcsusa.net](mailto:vnanda@pcsusa.net)

**T:** 404-301-1584



## Table of Contents

<b>Description of Solution</b>	<b>4</b>
Specifications	4
Multi-Tenancy Support	4
Scalability	4
Cloud Management	5
Managed Security Services	5
Prevention	6
Product Usability	7
Administration and Management Usability	8
Endpoint Protection Platform Suite	9
Operating Support	9
Data Management and Storage	10
Performance Management	10
Security	11
Data Management	12
Network	13
Compliance and Third-Party Certification	13
Configuration and Customization	15
Role Based Access	15
Integrations	16
Integrate with a SIEM	16
Identity and Access Management (IAM) Systems	16
Must connect to State SOC (CSOC)	16
SkyHelm Maintains Integration and Troubleshoots Issues	16
SLA for Solution	17
SLA for Training and Support	19
Implementation Plan	21
MDR SLA	23
DR Plan	27
<b>Experience and Service Capabilities</b>	<b>28</b>
Cybersecurity Expertise	28
About our 24/7 Security Operations Center (SkySOC)	29
Our Facilities and Systems Resiliency	30



Consulting Business	30
Relevant Past Performance	31
<b>Attachment A</b>	<b>32</b>
V. Waterfall Pricing	34
Vii. Value-Added Services	34
Managed Detection and Response (INCLUDED IN PRICING)	34
Achieving the 99.999% Uptime	35
Optional Added Services	36
On-Site Training	36
Managed & Monitored FortiSIEM	37
Forensics and Remediation Services	38
<b>Attachment B</b>	<b>40</b>
<b>Non-Disclosure Agreement</b>	<b>41</b>
<b>Partnerships (Subcontractors)</b>	<b>45</b>
<b>PCS and SkyHelm Partnership</b>	<b>45</b>
Services	46





## Description of Solution

This section will provide Documentation to describe the endpoint detection and response Solution.

### Specifications

#### Multi-Tenancy Support

FortiEDR supports multitenancy and role-based access control (RBAC). Multitenancy allows you to create multiple isolated tenants within a single FortiEDR environment. This can be useful for organizations that need to share a FortiEDR deployment with multiple customers or business units. RBAC allows you to define granular permissions for users and groups. This can help you to control who has access to what data and features.

To enable multitenancy in FortiEDR, you need to create a new tenant. You can do this by going to the Tenants page and clicking Create Tenant. You will need to provide a name for the tenant, a description, and a security profile. The security profile determines the level of access that the tenant will have to FortiEDR features.

Once you have created a tenant, you can add users and groups to it. You can do this by going to the Users page and clicking Add User. You will need to provide a username, a password, and a role. The role determines the level of access that the user will have to FortiEDR features.

FortiEDR supports the following roles:

- Admin: This role has full access to all FortiEDR features.
- User: This role has limited access to FortiEDR features.
- Guest: This role has very limited access to FortiEDR features.

#### Scalability

FortiEDR is scalable. It can be deployed in a variety of environments, from small businesses to large enterprises. FortiEDR can be scaled up by adding more FortiEDR appliances or by adding more capacity to existing appliances.

FortiEDR's scalability is achieved through a cloud-based management console that allows you to manage FortiEDR appliances from a central location.

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



## Cloud Management

Yes, FortiEDR is managed through a cloud environment.

## Managed Security Services

SkyHelm's Managed Security Services (MSS) utilizing FortiEDR provides comprehensive security for your organization. It includes:

- 24/7/365 monitoring and threat detection
- Incident response and remediation
- Compliance reporting
- Security consulting

FortiEDR is a next-generation endpoint detection and response (EDR) solution that provides visibility into all endpoint activity. It can detect and respond to threats that evade traditional security solutions, such as malware, ransomware, and advanced persistent threats (APTs).

SkyHelm's MSS utilizes FortiEDR to provide a comprehensive security solution for your organization. It includes the following technical details:

- FortiEDR is deployed on endpoints throughout your organization.
- FortiEDR collects data from endpoints, including process execution, file access, network traffic, and user activity.
- FortiEDR uses machine learning and artificial intelligence to analyze the data and detect threats.
- SkyHelm's security analysts monitor FortiEDR for threats and take action to respond to them.
- SkyHelm provides compliance reporting to help you meet your security requirements.
- SkyHelm offers security consulting to help you improve your security posture.

SkyHelm's MSS utilizing FortiEDR is a comprehensive security solution that can help you protect your organization from threats. It is a cost-effective way to get the security you need without the need to hire and train your own security team.

Here are some of the benefits of using SkyHelm's MSS utilizing FortiEDR:

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



- Reduced risk: SkyHelm's MSS can help you reduce the risk of cyberattacks by providing comprehensive security for your organization.
- Increased visibility: SkyHelm's MSS provides you with visibility into all endpoint activity, which can help you identify and respond to threats more quickly.
- Improved compliance: SkyHelm's MSS can help you meet your security requirements by providing compliance reporting.
- Reduced costs: SkyHelm's MSS is a cost-effective way to get the security you need without the need to hire and train your own security team.

## Prevention

FortiEDR Pre-execution Prevention (PEP) is a feature that can help to protect your organization from malware and other threats. PEP works by preventing malicious code from executing on your endpoints.

PEP uses a variety of techniques to detect and prevent malicious code, including:

- Static analysis: PEP analyzes the code of executable files before they are executed. This allows PEP to detect malicious code that is not yet known to FortiEDR.
- Dynamic analysis: PEP monitors the behavior of executable files while they are running. This allows PEP to detect malicious code that tries to evade static analysis.
- Machine learning: PEP uses machine learning to identify patterns of behavior that are associated with malicious code. This allows PEP to detect new and unknown threats.

PEP is a powerful tool that can help to protect your organization from malware and other threats. However, it is important to note that PEP is not a silver bullet. It is important to use other security measures, such as antivirus software and firewalls, in conjunction with PEP to provide comprehensive protection.

FortiEDR also has signature-based capabilities. Signature-based detection is a traditional method of detecting malware that relies on identifying known malicious code patterns. FortiEDR uses a variety of signature databases to detect known malware, including the Fortinet Threat Intelligence Feed, the FortiGuard Labs Threat Feed, and the Microsoft Malware Protection Center (MMPC) Threat Intelligence Feed.

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



Signature-based detection is a quick and effective way to detect known malware. However, it is not as effective at detecting new or unknown malware. This is because malware authors are constantly changing their code to evade detection.

FortiEDR combines signature-based detection with other detection methods, such as behavioral analysis and machine learning, to provide comprehensive protection against malware.

## Product Usability

FortiEDR is easy to use because it has a simple and intuitive user interface. The user interface is designed to be easy to navigate, even for users with no security experience.

FortiEDR also has a number of features that make it easy to use, including:

- A centralized management console: The FortiEDR management console allows you to manage all of your FortiEDR appliances from a single location.
- A drag-and-drop interface: The FortiEDR management console uses a drag-and-drop interface to make it easy to configure your FortiEDR appliances.
- A built-in help system: The FortiEDR management console includes a built-in help system that provides detailed information on how to use FortiEDR.

FortiEDR is also easy to deploy. The FortiEDR deployment process is simple and straightforward, and it can be completed in a few minutes.

Here are some of the benefits of using FortiEDR in the context of being easy to use:

- Reduced complexity: FortiEDR's ease of use can help you reduce the complexity of your security environment.
- Increased productivity: FortiEDR's ease of use can help you increase your productivity by reducing the time it takes to manage your security environment.
- Improved security: FortiEDR's ease of use can help you improve your security posture by making it easier to deploy and manage your security solutions.



## Administration and Management Usability

The FortiEDR administration console is easy to use and provides a centralized view of your FortiEDR deployment. The console allows you to manage all aspects of your FortiEDR environment, including devices, policies, and events. The console is also highly scalable and can be used to manage large FortiEDR deployments.

The FortiEDR agent is lightweight and has a low performance impact. This is due to FortiEDR's unique Kernel Replacement technology. Kernel Replacement allows the FortiEDR agent to run in the kernel space, which is the most privileged space on the endpoint. This allows the FortiEDR agent to collect data and respond to threats without impacting the performance of the endpoint.

Here are some of the technical details about how FortiEDR's agent is lightweight and has a low performance impact:

- The FortiEDR agent is a small, lightweight binary that is easy to deploy and manage.
- The FortiEDR agent runs in the kernel space, which is the most privileged space on the endpoint.
- The FortiEDR agent only collects the data that is necessary to detect and respond to threats.
- The FortiEDR agent uses a variety of techniques to minimize its impact on the endpoint, such as using asynchronous processing and thread pooling.

***FortiEDR's unique Kernel Replacement technology*** is what allows the FortiEDR agent to run in the kernel space and collect data without impacting the performance of the endpoint. Kernel Replacement is a complex technology, but it is essential for FortiEDR to be able to provide its advanced security features.

Here are some of the benefits of using FortiEDR's lightweight agent and low performance impact:

- **Reduced resource consumption:** The FortiEDR agent consumes very few resources, which helps to preserve the performance of your endpoints.



- Improved security: The FortiEDR agent can collect data and respond to threats without impacting the performance of your endpoints, which helps to improve your security posture.
- Reduced complexity: The FortiEDR agent is easy to deploy and manage, which helps to reduce the complexity of your security environment.

## Endpoint Protection Platform Suite

FortiEDR's Protection Platform Suite is a comprehensive set of security features that can help to protect your organization from a wide range of threats. The suite includes the following features:

- Endpoint firewall: The endpoint firewall provides protection against network-based threats, such as malware and ransomware.
- Device and application controls: The device and application controls provide granular control over the devices and applications that are used on your endpoints.
- Application inventorying: The application inventorying feature provides a comprehensive view of the applications that are installed on your endpoints.
- Signature matching: The signature matching feature provides protection against known threats by comparing file signatures to a database of known threats.
- Vulnerability detection: The vulnerability detection feature scans your endpoints for known vulnerabilities and provides recommendations for remediation.
- Sandboxing: The sandboxing feature allows you to run suspicious files in a controlled environment to analyze them for malicious behavior.

These features work together to provide comprehensive protection for your endpoints. While FortiEDR does not have a mail plugin, it is not needed due to its kernel architecture, freeing up additional computational resources!

## Operating Support

FortiEDR supports the following operating systems:

- Windows 10, 11, and Server 2016 and later
- macOS High Sierra, Mojave, Catalina, Big Sur, and Monterey
- Linux distributions based on Red Hat Enterprise Linux (RHEL) 6.8, 7.2, 7.3, 7.4, 7.5, 7.6, and 7.7, and Ubuntu 16.04.5, 16.04.6, 18.04.1, and 18.04.2



FortiEDR also supports a limited number of other operating systems, such as Chrome OS and FreeBSD.

FortiEDR does not support any Mobile OS, or any ARM architecture processors.

FortiEDR can be deployed on physical or virtual endpoints. The FortiEDR agent is lightweight and has a low performance impact, so it can be deployed on endpoints with limited resources.

### Data Management and Storage

FortiEDR keeps logs for a minimum of 90 days, but you can configure it to keep logs for up to 1 year. The logs are stored in the FortiEDR cloud and can be accessed by your FortiEDR administrator. However, data can also be sent to a SIEM tool for additional storage. Additionally, SkyHelm is SOC2 compliant as is Fortinet. All customer data is backed up and stored securely.

### Performance Management

FortiEDR has a comprehensive alerting system that can help you to identify and respond to threats. FortiEDR can generate alerts for a variety of events, including:

- File system access: FortiEDR can generate alerts for suspicious file system access, such as attempts to access files that are known to be malicious.
- Network connections: FortiEDR can generate alerts for suspicious network connections, such as attempts to connect to known malicious IP addresses.
- Process execution: FortiEDR can generate alerts for suspicious process execution, such as attempts to execute known malicious files.
- Registry changes: FortiEDR can generate alerts for suspicious registry changes, such as attempts to make changes to the registry that could be used to gain unauthorized access.
- Device and application controls: FortiEDR can generate alerts for violations of device and application controls, such as attempts to install unauthorized software or to connect to unauthorized devices.
- Vulnerability detection: FortiEDR can generate alerts for vulnerabilities that are found on your endpoints. These alerts can help you to prioritize remediation efforts and to protect your endpoints from exploitation.

FortiEDR can send alerts to a variety of destinations, including:

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



- Email: FortiEDR can send alerts to your email address.
- SNMP: FortiEDR can send alerts to an SNMP trap receiver.
- Syslog: FortiEDR can send alerts to a syslog server.
- Custom integrations: FortiEDR can integrate with a variety of third-party systems to send alerts.

We can configure FortiEDR to generate alerts for specific events and to send alerts to specific destinations. This allows you to customize the alerting system to meet your specific needs.

SkyHelm and PCS will utilize a helpdesk ticketing system to track issues to completion.

## Security

FortiEDR's web hosted platform is designed to be secure and reliable. The platform is hosted in Fortinet's secure data centers, which are protected by a variety of security measures, including:

- Physical security: The data centers are located in secure facilities that are protected by 24/7 security guards and video surveillance.
- Network security: The data centers are connected to the internet through a secure network that is protected by a variety of firewalls and intrusion detection systems.
- Environmental security: The data centers are equipped with environmental controls that protect the equipment from fire, flood, and other hazards.
- Personnel security: Fortinet employees who have access to the data centers are subject to background checks and security clearances.

In addition to the physical and network security measures, Fortinet also has a comprehensive set of security policies and procedures in place to protect the FortiEDR web hosted platform. These policies and procedures cover a variety of areas, including:

- Access control: Access to the data centers and the FortiEDR platform is restricted to authorized personnel only.
- Data encryption: All data stored on the FortiEDR platform is encrypted using industry-standard encryption algorithms.
- Backup and recovery: The FortiEDR platform is backed up regularly and can be restored in the event of a disaster.
- Auditing: Fortinet conducts regular audits of the FortiEDR web hosted platform to ensure that it is meeting its security requirements.





Fortinet also publishes a variety of security reports and attestations to demonstrate its commitment to security. These reports include:

- SOC 2 Type 2 Report: This report attests to Fortinet's compliance with the AICPA's SOC 2 Type 2 reporting framework.
- ISO/IEC 27001:2013 Certification: This certification attests to Fortinet's compliance with the ISO/IEC 27001:2013 information security standard.
- PCI DSS 3.2 Compliance: Fortinet is compliant with the PCI DSS 3.2 security standard.

The FortiEDR web hosted platform is a secure and reliable solution for organizations that need to protect their endpoints from threats. The platform is hosted in Fortinet's secure data centers and is protected by a comprehensive set of security policies and procedures. Fortinet also publishes a variety of security reports and attestations to demonstrate its commitment to security.

SkyHelm is also SOC2 compliant.

## Data Management

Fortinet FortiEDR uses a variety of security measures to protect the confidentiality, integrity, and availability of data in transit. These security measures include:

- Encryption: FortiEDR uses industry-standard encryption algorithms to protect data in transit. The encryption algorithms used by FortiEDR include AES, RSA, and SHA-256.
- Transport Layer Security (TLS): FortiEDR uses TLS to secure communications between FortiEDR devices and the FortiEDR cloud. TLS is a cryptographic protocol that provides confidentiality, integrity, and authentication for data in transit.
- Firewalls: FortiEDR uses firewalls to restrict access to the FortiEDR cloud. The firewalls used by FortiEDR are configured to only allow authorized traffic to reach the FortiEDR cloud.
- Intrusion Detection Systems (IDS): FortiEDR uses IDS to detect malicious traffic that may be attempting to exploit vulnerabilities in the FortiEDR cloud. The IDS used by FortiEDR is configured to identify and block malicious traffic.
- Web Application Firewalls (WAFs): FortiEDR uses WAFs to protect the FortiEDR cloud from web-based attacks. The WAF used by FortiEDR is configured to block malicious traffic and to prevent unauthorized access to the FortiEDR cloud.



- Data Loss Prevention (DLP): FortiEDR uses DLP to prevent sensitive data from being leaked from the FortiEDR cloud. The DLP used by FortiEDR is configured to identify and block sensitive data from being exfiltrated from the FortiEDR cloud.

These security measures help to protect the confidentiality, integrity, and availability of data in transit to and from the FortiEDR cloud.

In addition to the security measures listed above, FortiEDR also uses a variety of other security measures to protect data at rest. These security measures include:

- Data encryption: FortiEDR encrypts data at rest using industry-standard encryption algorithms. The encryption algorithms used by FortiEDR include AES, RSA, and SHA-256.
- Data loss prevention (DLP): FortiEDR uses DLP to prevent sensitive data from being leaked from FortiEDR devices. The DLP used by FortiEDR is configured to identify and block sensitive data from being exfiltrated from FortiEDR devices.
- Data access control: FortiEDR uses data access control to restrict access to sensitive data. Data access control is configured to only allow authorized users to access sensitive data.
- Vulnerability management: FortiEDR uses vulnerability management to identify and patch vulnerabilities in FortiEDR devices. Vulnerability management is configured to scan FortiEDR devices for vulnerabilities and to automatically patch vulnerabilities that are identified.

## Network

As the solution is cloud hosted, it has no issues using the supported network types.

## Compliance and Third-Party Certification

FortiEDR web hosted is compliant with GDPR, CJIS, HIPAA, PII, SOC2, and ISO 27001.

- GDPR: The General Data Protection Regulation (GDPR) is a European Union regulation that sets forth strict requirements for the processing of personal data. FortiEDR web hosted is compliant with the GDPR by design and by default. FortiEDR web hosted includes a number of features that help to protect personal data, such as encryption, access control, and audit logging.

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



- CJIS: The Criminal Justice Information Services (CJIS) Act is a United States federal law that sets forth security requirements for the processing of criminal justice information. FortiEDR web hosted is compliant with the CJIS Act by design and by default. FortiEDR web hosted includes a number of features that help to protect criminal justice information, such as encryption, access control, and audit logging.
- HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) is a United States federal law that sets forth security requirements for the processing of protected health information (PHI). FortiEDR web hosted is compliant with HIPAA by design and by default. FortiEDR web hosted includes a number of features that help to protect PHI, such as encryption, access control, and audit logging.
- PII: Personally identifiable information (PII) is any information that can be used to identify an individual, such as their name, address, or Social Security number. FortiEDR web hosted is designed to protect PII by encrypting it at rest and in transit. FortiEDR web hosted also includes a number of features that help to prevent unauthorized access to PII, such as access control and audit logging.
- SOC2: The System and Organization Controls (SOC) 2 is a set of auditing standards that are designed to assess the security, availability, and confidentiality of an organization's information systems. FortiEDR web hosted is compliant with SOC 2 by design and by default. FortiEDR web hosted includes a number of features that help to protect an organization's information systems, such as encryption, access control, and audit logging.
- ISO 27001: The International Organization for Standardization (ISO) 27001 is an international standard that sets forth requirements for an information security management system (ISMS). FortiEDR web hosted is compliant with ISO 27001 by design and by default. FortiEDR web hosted includes a number of features that help to protect an organization's information security, such as encryption, access control, and audit logging.



## Configuration and Customization

Due to FortiEDR's simplicity and ease of use, there aren't many customizations with the UI. That said, there are several points of configuration available. Including the ability to monitor and control USB devices.

## Role Based Access

FortiEDR provides role-based access control (RBAC) to allow administrators to control who has access to FortiEDR and what they can do with it. RBAC is based on the principle of least privilege, which means that users should only be given access to the resources that they need to do their job.

FortiEDR RBAC has three main components: roles, users, and permissions.

- Roles: Roles define the permissions that users have in FortiEDR. FortiEDR comes with a number of pre-defined roles, such as administrator, analyst, and viewer. Administrators have the most permissions, analysts can view and analyze data, and viewers can only view data.
- Users: Users are the people who have access to FortiEDR. FortiEDR can be configured to allow users to log in with their Active Directory credentials or with a local account.
- Permissions: Permissions define what users can do in FortiEDR. Permissions can be granted to roles or to individual users. For example, the "View Data" permission allows users to view data in FortiEDR.

FortiEDR RBAC can be used to control access to a variety of FortiEDR resources, including:

- Devices: FortiEDR devices can be controlled using RBAC. For example, administrators can use RBAC to grant users the ability to view, modify, or delete device configurations.
- Policies: FortiEDR policies can be controlled using RBAC. For example, administrators can use RBAC to grant users the ability to view, modify, or delete policies.
- Data: FortiEDR data can be controlled using RBAC. For example, administrators can use RBAC to grant users the ability to view, modify, or delete data.

FortiEDR RBAC is a powerful tool that can be used to improve the security of FortiEDR deployments. By using RBAC, administrators can ensure that only authorized users have access to FortiEDR and that they can only do what they need to do.



## Data Export

FortiEDR can export data in a variety of formats, including:

- CSV: CSV is a comma-separated value format that is commonly used for data export.
- JSON: JSON is a JavaScript Object Notation format that is commonly used for data exchange.
- XML: XML is an Extensible Markup Language format that is commonly used for data exchange.
- SIEM: FortiEDR can export data in a format that is compatible with SIEM systems.

## Integrations

### ***Integrate with a SIEM***

FortiEDR can send data to a SIEM tool using a variety of methods, including:

- SIEM-specific connectors: FortiEDR comes with a variety of connectors that allow it to send data to specific SIEM tools. These connectors are pre-configured and tested to work with FortiEDR and the SIEM tool.
- Generic connectors: FortiEDR also comes with a generic connector that can be used to send data to any SIEM tool. The generic connector is not pre-configured for any specific SIEM tool, but it can be configured to work with any SIEM tool that supports the CEF (Common Event Format) or JSON (JavaScript Object Notation) data formats.
- RESTful API: FortiEDR also has an API that can be used to send data to a SIEM tool. The API is a powerful tool that can be used to send data to any SIEM tool, regardless of whether or not it has a pre-configured connector for FortiEDR.

### ***Identity and Access Management (IAM) Systems***

FortiEDR can work with IAM systems. FortiEDR can be configured to integrate with a variety of IAM systems, including Active Directory, Okta, and OneLogin.

### ***Must connect to State SOC (CSOC)***

FortiEDR will be available to the State SOC and can be fed into their SIEM solution.

### ***SkyHelm Maintains Integration and Troubleshoots Issues***



## SLA for Solution

FortiEDR maintained an uptime of 99.999% in 2020-2021. While in 2022, the uptime dipped slightly to 99.99%. In order to achieve 99.999% we have datacenters in multiple, geographically dispersed U.S. locations hosting multiple redundant and load balanced copies of FortiEDR. Monitored by our U.S. based employees.

FortiEDR uses a variety of techniques to maintain its high uptime, including:

- Redundancy: FortiEDR is deployed in a redundant configuration, with multiple appliances providing coverage for each endpoint in multiple datacenters. This helps to ensure that there is always an appliance available to protect endpoints, even if one appliance fails.
- Load balancing: FortiEDR is deployed in a load-balanced configuration, with multiple appliances sharing the workload of protecting endpoints. This helps to improve performance and can also help to prevent outages if one appliance fails.
- Failover: FortiEDR is configured to automatically fail over to a backup appliance or datacenter if the primary appliance or datacenter becomes unavailable. This helps to ensure that endpoint protection is always available, even if there is an outage.

Here is a draft SLA for 99.999% uptime for FortiEDR:

*Service Level Agreement*

*Customer: [Customer Name]*

*Service Provider: PCS*

*Service: FortiEDR*

*Uptime: 99.999%*

*Penalty: For each percentage point below 99.999%, PCS will credit the customer that percentage off of the monthly bill.*

*Term: This SLA is for a period of one year.*

*Renewal: This SLA will automatically renew for one-year periods unless either party provides written notice of termination at least 30 days prior to the end of the current term.*

*Support: PCS will provide 24/7 support for FortiEDR.*

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



*Reporting: PCS will provide monthly reports on FortiEDR uptime.*

*Resolution: If FortiEDR is not available for 99.999% of the time, PCS will work to resolve the issue as quickly as possible. If the issue is not resolved within 24 hours, PCS will credit the customer for the percentage of time that FortiEDR was not available.*

*Waiver: PCS may waive this SLA if the unavailability of FortiEDR is due to circumstances beyond PCS's control, such as a natural disaster or a third-party outage.*

*Indemnification: PCS will indemnify and hold harmless the customer from any and all claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or in connection with PCS's breach of this SLA.*

*Governing Law: This SLA will be governed by and construed in accordance with the laws of the State of California.*

*Entire Agreement: This SLA **does not** constitute the entire agreement between the parties with respect to the subject matter hereof.*

*Severability: If any provision of this SLA is held to be invalid or unenforceable, such provision will be struck from this SLA and the remaining provisions will remain in full force and effect.*

*Assignment: This SLA may not be assigned by either party without the prior written consent of the other party.*

*Notices: All notices and other communications hereunder will be in writing and will be deemed to have been duly given when delivered in person, upon the first business day following deposit in the United States mail, postage prepaid, certified or registered, return receipt requested, addressed as follows:*

*If to Customer:  
[Customer Name]*

*[Address]*

*If to PCS:*

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



PCS

*[Address]*

*or to such other address as either party may designate in writing from time to time.*

*Waiver: No waiver of any provision of this SLA will be effective unless in writing and signed by both parties. No waiver of any provision of this SLA will operate or be construed as a waiver of any other provision of this SLA, whether or not similar.*

*Headings: The headings in this SLA are for convenience only and will not affect its interpretation.*

*Counterparts: This SLA may be executed in one or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.*

*Binding Effect: This SLA will be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.*

## SLA for Training and Support

Below is a draft SLA for training and support to be conducted by PCS for FortiEDR:

*Service Level Agreement*

*Customer: [Customer Name]*

*Service Provider: PCS*

*Service: FortiEDR*

*Training:*

*Initial training will take place within 10 days of onboarding.*

*Additional training requests will be scheduled within 5 business days of the original request.*

*Support:*

*24/7 support will be provided.*

*Response time for all support requests will be 30 minutes.*

*Term: This SLA is for a period of one year.*

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution





*Renewal: This SLA will automatically renew for one-year periods unless either party provides written notice of termination at least 30 days prior to the end of the current term.*

*Resolution: If a support request is not resolved within 30 minutes, PCS will work to resolve the issue as quickly as possible.*

*Waiver: PCS may waive this SLA if the unavailability of FortiEDR is due to circumstances beyond PCS's control, such as a natural disaster or a third-party outage.*

*Indemnification: PCS will indemnify and hold harmless the customer from any and all claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or in connection with PCS's breach of this SLA.*

*Governing Law: This SLA will be governed by and construed in accordance with the laws of the State of California.*

*Entire Agreement: This SLA **does not constitute** the entire agreement between the parties with respect to the subject matter hereof.*

*Severability: If any provision of this SLA is held to be invalid or unenforceable, such provision will be struck from this SLA and the remaining provisions will remain in full force and effect.*

*Assignment: This SLA may not be assigned by either party without the prior written consent of the other party.*

*Notices: All notices and other communications hereunder will be in writing and will be deemed to have been duly given when delivered in person, upon the first business day following deposit in the United States mail, postage prepaid, certified or registered, return receipt requested, addressed as follows:*

*If to Customer:*

*[Customer Name]*

*[Address]*



*If to PCS:*

*PCS*

*[Address]*

*or to such other address as either party may designate in writing from time to time.*

*Waiver: No waiver of any provision of this SLA will be effective unless in writing and signed by both parties. No waiver of any provision of this SLA will operate or be construed as a waiver of any other provision of this SLA, whether or not similar.*

*Headings: The headings in this SLA are for convenience only and will not affect its interpretation.*

*Counterparts: This SLA may be executed in one or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.*

*Binding Effect: This SLA will be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.*

## Implementation Plan

Below is a draft implementation plan for deploying FortiEDR:

*Implementation Plan*

*Customer: [Customer Name]*

*Service Provider: PCS*

*Service: FortiEDR*

*Timeline: 30 days*

*Tasks:*

*1. Day 1:*

- Customer and PCS will meet to discuss the implementation plan.*
- Customer will provide PCS with access to the network.*
- PCS will install the FortiEDR appliances.*

*2. Day 2:*

- PCS will configure the FortiEDR appliances.*

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



- *PCS will create a training plan for the customer.*
- 3. *Day 3:*
  - *PCS will begin training the customer on how to use the FortiEDR appliances.*
- 4. *Days 4-28:*
  - *PCS will continue training the customer on how to use the FortiEDR appliances.*
  - *PCS will ensure deployment of agents on devices.*
  - *PCS will monitor the FortiEDR appliances for any issues.*
- 5. *Day 29:*
  - *PCS will provide the customer with a final report on the implementation.*

#### *Responsibilities:*

- *Customer:*
  - *Provide PCS with access to the network for installation.*
  - *Attend training sessions.*
  - *Provide feedback to PCS on the implementation.*
- *PCS:*
  - *Install the FortiEDR appliances.*
  - *Configure the FortiEDR appliances.*
  - *Create a training plan for the customer.*
  - *Conduct training sessions for the customer.*
  - *Monitor the FortiEDR appliances for any issues.*
  - *Provide a final report on the implementation.*

#### *Training:*

- *The training will be conducted remotely.*
- *The training will cover the following topics:*
  - *FortiEDR overview*
  - *FortiEDR configuration*
  - *FortiEDR monitoring*
  - *FortiEDR troubleshooting*

#### *Contact Information:*

- *Customer:*



- *Name: [Customer Name]*
- *Email: [Customer Email]*
- *Phone: [Customer Phone Number]*
- **PCS:**
  - *Name: [PCS Name]*
  - *Email: [PCS Email]*
  - *Phone: [PCS Phone Number]*

#### *Project Manager:*

- *The project manager will be [Project Manager Name].*
- *The project manager will communicate the ongoing status of the implementation plan to the customer on a weekly basis.*

#### *Technical Details:*

*FortiEDR is deployed in a distributed fashion, with one or more FortiEDR appliances deployed at each location that needs to be protected. The FortiEDR appliances communicate with each other using a secure tunnel, and they can be managed from a central FortiEDR management console.*

*The FortiEDR appliances collect data from endpoints, such as computers, servers, and mobile devices, and they use this data to detect and prevent threats. FortiEDR can also be used to investigate security incidents and to respond to threats.*

*FortiEDR is a powerful tool that can be used to improve the security of an organization. By deploying FortiEDR, organizations can make it more difficult for attackers to gain access to sensitive data and systems.*

## **MDR SLA**

Below is a draft SLA for Managing Alerts within FortiEDR. The SLA includes that alerts will be reviewed within 15 minutes and handled within 30 minutes. All alerts are handled by PCS' SOC through SkyHelm.

#### *Service Level Agreement*

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



*Service Name: Managing Alerts within FortiEDR*

*Service Provider: PCS*

*Customer: [Customer Name]*

*Effective Date: [Start Date]*

*Term: [Term Length]*

### *1. Scope of Service*

*PCS agrees to provide the Managing Alerts within FortiEDR service to the Customer in accordance with the terms and conditions of this SLA. The Managing Alerts within FortiEDR service includes the following:*

- Review of all alerts within 15 minutes of being generated.*
- Handling of all alerts within 30 minutes of being generated.*

### *2. Service Levels*

*PCS will review all alerts within 15 minutes of being generated.*

*PCS will handle all alerts within 30 minutes of being generated.*

### *3. Service Credits*

*If PCS fails to meet the service levels set forth in this SLA, then the Customer will be entitled to a service credit. The amount of the service credit will be equal to the percentage of time that the service was unavailable multiplied by the monthly bill.*

### *4. Reporting*

*PCS will provide the Customer with monthly reports that track the availability of the Managing Alerts within FortiEDR service. The reports will include the total amount of time that the service was unavailable and the percentage of time that the service was unavailable.*

### *5. Remediation*

**RFQ #: DMS-22/23-155**

**Endpoint Detection and Response Solution**



*If the Managing Alerts within FortiEDR service is unavailable, then PCS will work to restore the service as quickly as possible. PCS will also investigate the cause of the outage and take steps to prevent it from happening again.*

#### *6. Dispute Resolution*

*If there is a dispute between the Customer and PCS regarding the availability of the Managing Alerts within FortiEDR service, then the dispute will be resolved through mediation. If mediation is unsuccessful, then the dispute will be resolved through arbitration.*

#### *7. Severability*

*If any provision of this SLA is held to be invalid or unenforceable, then the remaining provisions will remain in full force and effect.*

#### *8. Entire Agreement*

*This SLA **does not constitute** the entire agreement between the Customer and PCS regarding the provision of the Managing Alerts within FortiEDR service.*

#### *9. Governing Law*

*This SLA will be governed by and construed in accordance with the laws of the State of [State].*

#### *10. Notices*

*All notices and other communications under this SLA will be in writing and will be deemed to have been duly given when delivered in person, upon the first business day following deposit in the United States mail, postage prepaid, certified or registered, return receipt requested, addressed as follows:*

*If to the Customer:  
[Customer Name]*

*[Customer Address]*



*If to PCS:  
PCS*

*[PCS Address]*

*or to such other address as either party may designate in writing from time to time.*

#### *11. Waiver*

*No waiver of any provision of this SLA will be effective unless in writing and signed by both parties.*

#### *12. Successors and Assigns*

*This SLA will be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.*

#### *13. Headings*

*The headings in this SLA are for convenience only and will not affect its interpretation.*

#### *14. Counterparts*

*This SLA may be executed in one or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.*

#### *Additional Details*

- *Alerts will be reviewed and handled by PCS' SOC through SkyHelm.*
- *SkyHelm is a cloud-based security information and event management (SIEM) platform that provides PCS with the ability to monitor and analyze IT security events from across the customer's environment.*
- *SkyHelm uses machine learning and artificial intelligence to identify and prioritize security threats, and to automate the response to these threats.*
- *This ensures that all alerts are reviewed and handled in a timely manner, and that any security threats are quickly identified and mitigated.*

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



## DR Plan

*PCS and SkyHelm attests that we have implemented suitable controls to protect Customer data consumed by FortiEDR. These controls are commensurate with the classification of the data, as defined in Chapter 60GG-2, F.A.C.*

### *Technical Security Controls*

*The following technical security controls are in place to protect Customer data consumed by FortiEDR:*

- *Data encryption*
- *Access control*
- *Auditing*
- *Incident response*
- *Disaster recovery*

### *Data Encryption*

*All Customer data stored in FortiEDR is encrypted using industry-standard encryption algorithms. This ensures that the data is protected from unauthorized access, even if the FortiEDR system is compromised.*

### *Access Control*

*Access to FortiEDR is restricted to authorized personnel only. All users must have a valid username and password to access the system. Additionally, user access is logged and monitored to track any suspicious activity.*

### *Auditing*

*SkyHelm audits all system activity. This includes all logins, changes to data, and access to sensitive files. The audit logs are reviewed on a regular basis to identify any potential security threats.*

### *Incident Response*

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution





*PCS has a comprehensive incident response plan in place to deal with any security incidents that may occur. The plan includes steps to identify, contain, and mitigate any incidents. Additionally, the plan includes steps to notify affected customers and to restore service as quickly as possible.*

#### *Disaster Recovery*

*PCS has a disaster recovery plan in place to ensure that Customer data is protected in the event of a disaster. The plan includes steps to back up data on a regular basis, to store backups in multiple locations, and to restore data in the event of a disaster.*

#### *Daily Backups*

*FortiEDR is backed up on a daily basis. The backups are stored in a secure location off-site.*

#### *Multiple Archived Copies*

*Multiple archived copies of Customer data are stored in secure locations off-site. This ensures that Customer data is protected in the event of a disaster.*

## Experience and Service Capabilities

The below is documentation describing any experience providing the Solution, or similar Solution, on a statewide basis or across a large geographic region.

### Cybersecurity Expertise

PCS and SkyHelm are established national cybersecurity experts. We have a research team that has developed customized honeypots, conducted covert dark web intelligence collection, and participated in proactive white hat hacking activities. SkyHelm has reported vulnerabilities to over 24 different cybersecurity organizations including MS-ISAC, DOD, FBI, and WaterISAC, to name a few.

We are not only following cybersecurity sources of information to stay up-to-date on the latest phishing attacks or vulnerabilities, but in some cases, we are the source of information notifying the rest of the world about the latest cybersecurity threats. SkyHelm was the first organization to share information out about the SolarWinds Orion Security Vulnerability (AKA



SunBurst/SolarGate) to Information and Sharing Analysis Centers operated by the electric industry, DHS, US-CERT, DOD, DOE, Water Utilities, and governmental organizations (MS-ISAC) (Ref posting ID 128804 submitted organizationally by Travis Cleek, TLP Green). SkyHelm also has reported on other vulnerabilities such as the infamous Sonicwall VPN vulnerabilities from October.

The screenshot shows the E-ISAC (Electricity Information Sharing and Analysis Center) website. The page title is "Cyber Bulletin Detail" for "SonicWall VPN Vulnerabilities". The posting ID is 127525, and it was added and modified on 10/16/2020 at 10:20 PM EDT. The author is Travis Cleek, an E-ISAC AOO Member. The bulletin has a 5-star rating. Action buttons include "Edit Cyber Bulletin", "Delete Cyber Bulletin", and "Report as Objectionable". The description states that SkyHelm, a critical infrastructure focused cybersecurity firm, is working with utility customers to patch their pre-existing SonicWall firewalls. A list of related entities is provided: International (other ISACs, CERTs), International AOOs, and MS-ISAC.

*(Image taken from a Publicly Shareable, TLP White, Vulnerability)*

Additionally, SkyHelm regularly publishes cybersecurity blog articles. Articles discuss topics ranging from remote access dangers relating to ransomware to industry leading discussions on password policies.

### About our 24/7 Security Operations Center (SkySOC)

We are a team of certified and experienced cybersecurity professionals. All SOC employees must pass the Network Security Exams level 3 to become NSE3 certified. Additionally, we have SOC employees who have obtained their NSE5 certifications. Due to the sensitive nature and criticality



of our monitored customers, all employees must go through a thorough a rigorous background check process to ensure we are doing our part in keeping America safe.

## Our Facilities and Systems Resiliency

To get to our NOC/SOC area in Oklahoma City, you have to enter through the building's access control at the front door, the elevator, and entry into our offices. The building only allows initial access during regular business hours, otherwise you must use an RFID badge to gain entry. Our floor requires that you badge in, everytime, to enter our office area. There is only a small group of people allowed access into our server room. Our NOC/SOC area requires a password or badge and a fingerprint in order to gain access. Everything is logged and all entries/exits are recorded. There are security cameras watching every entry and exit from the NOC/SOC area.

Due to our work with critical infrastructure our NOC/SOC is designed to exceed National Energy Regulatory Commission (NERC) critical infrastructure protection (CIP) compliance. Further we follow a comprehensive cybersecurity framework when we approach our own network security and design. Our goal was to take the best of the National Institute of Standards in Technology (NIST) cybersecurity guidelines and Centers for Internet Security (CIS) Top 20 to create a more cybersecure environment along with required NERC CIP regulatory compliance. Further, we are in compliance with recommendations from the Midwest Reliability Organization, Western Electricity Coordinating Council, and the State Emergency Response Commission (SERC) Reliability Corporation.

Our systems run in a primary datacenter in Oklahoma City. We have backups that run nightly, that are stored offsite in immutable storage, with failover capabilities to our offices in OKC or Denver. Right now, due to COVID-19 we're operating in one of our many emergency operation configurations. We are able to quickly implement several remote solutions including distancing, which we are doing now. We can also spin up operations from one of our secondary locations. We have a 24 hour battery backup solution and a generator on standby. This is more than enough time to allow us to fail-over to a backup site or redeploy in a new configuration.

## Consulting Business

We take a similar approach to consulting as we do when our team is building 9-1-1 emergency communication centers, working with police departments, or ensuring the safe delivery of power to over 340,000 people. Our philosophy of systems design and troubleshooting is centered in a deep understanding of the environment of application. Keeping an awareness of business needs, we utilize our most senior engineers to architect industry-leading designs focused on safety and reliability. In using senior engineers, we have unrivaled, comprehensive knowledge of how



technologies will function and react to their applied environments. We focus on creating and building the most dynamic and robust systems possible. In the utilities sector we commonly see rugged and remote application environments. Knowing that we need to provide 100% uptime we build multiple redundancies to keep connectivity to each device. We know cybersecurity and are perpetually cognizant of the risks, what data needs to be protected, and how we can best provide for that protection. We make sure we are meeting these needs by understanding the environments of application.

### Relevant Past Performance

The PCS team is no stranger to work with municipalities and government agencies. Some of the team members have worked in law enforcement technology. Building a state-wide information sharing system that was used by over 380 local, county, state, and federal public safety agencies. Plus, other leaders within our organization have a management background in utilities. Our team has a unique understanding of the complexities and requirements that county governments face with technology and cybersecurity.

Our team has worked on a number of engagements for customers involving the translation of complex compliance matrices into easy to understand and implement policies. A recent engagement we were engaged in for an Electric Generation and Transmission Cooperative in Texas involved mapping NIST CSF, NERC CIP and Insurance Covenants into policies. We then assisted the organization with building those policies and led the effort to identify the gaps in their current environment along with remediation projects to ensure that their organization was fully compliant with the applicable standards, compliance requirements and covenants.

Further, PCS/SkyHelm have been engaged directly with electric utilities and municipalities over the last 4 years in IP network design, cybersecurity design, 24/7 network & security operations monitoring, and systems design & implementation. Through this we have been highly successful in building a redundant, recoverable network and security infrastructure that is designed to allow continuous operation. Our project team has thousands of hours of experience working with the critical infrastructure networks. We are well positioned to leverage the core knowledge gained from current deployments for utilities, municipalities, and law enforcement to provide comprehensive cybersecurity services.



## Attachment A

### ATTACHMENT A PRICE SHEET

#### I. Alternate Contract Source (ACS)

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

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

#### II. Pricing Instructions

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

#### III. Pricing

Initial Term Pricing (Years 1-3)		
Item No.	Description	Rate Per Device
1	<p><b>Initial Software Year</b> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> <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>	\$ <b><u>\$56.99</u></b>
2	<p><b>Subsequent Software Year</b> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> <li>• <b>ongoing training</b></li> <li>• integration maintenance</li> <li>• support services</li> </ul>	\$ <b><u>\$53.11</u></b>

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



Optional Renewal Term Pricing (Years 4-6)		
Item No.	Description	Rate Per Device
1	<p><b>Initial Software Year</b> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> <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>	\$ <u><b>\$53.11</b></u>
2	<p><b>Subsequent Software Year</b> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> <li>• <b>ongoing training</b></li> <li>• integration maintenance</li> <li>• support services</li> </ul>	\$ <u><b>\$53.11</b></u>

#### 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
FC1-10-FEDR1-377-01-12	FortiEDR-25 FortiEDR Discover, Protect	\$2,550.00	\$2,167.50
FP-10-MDR-FRNSCS	FortiEDR Managed Detect and Respond	\$400.00	\$388.00

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	SKU Description	Market Price	ACS Price
FC1-10-FEDR1-377-01-12	FortiEDR-25 FortiEDR Discover, Protect	\$2,550.00	\$2,167.50



## V. Waterfall Pricing

Managed FortiEDR Pricing		
Devices	Subsequent Pricing	Initial Pricing
0-1000	\$53.11	\$56.99
1001-2000	\$49.23	\$53.11
2001-3000	\$45.35	\$49.23
3001-5000	\$42.48	\$45.35
5001+	\$41.49	\$42.48

Additional products or services offered to state agencies at a minimum of a 3% discount.

## Vii. Value-Added Services

### Managed Detection and Response (INCLUDED IN PRICING)

We made the decision to offer our low price while including the U.S. based Security Operations Center (SOC) team to manage the solution. While individual customers will have full administrative access to the solution, our U.S. team is there to respond and answer any questions 24/7/365. Our already low pricing already **includes** all the MDR features listed above that were “optional” at no additional cost!

- **Enhanced Threat Detection:** A Fully Managed FortiEDR solution with EDR (Endpoint Detection and Response) capabilities offers advanced threat detection mechanisms. It continuously monitors endpoints for any suspicious activity, detecting potential threats and indicators of compromise in real-time.
- **Rapid Incident Response:** With EDR response capabilities, the FortiEDR solution enables swift incident response. It provides your administrators and our 27/7 US SOC (Security Operations Center) with actionable insights and automated response options, allowing them to quickly contain and remediate security incidents, minimizing or even eliminating the potential impact of a breach.
- **Proactive Threat Hunting:** FortiEDR's EDR response empowers administrators and our 24/7 SOC to conduct proactive threat hunting. It allows for in-depth analysis of endpoint activities, searching for hidden threats or signs of advanced persistent threats (APTs) that may have evaded traditional security measures. This proactive approach helps identify and eliminate threats before they can cause significant damage.
- **Forensic Investigation:** The EDR response functionality within FortiEDR enables detailed forensic investigation. It provides comprehensive visibility into endpoint activities, including the ability to



track and analyze the entire attack chain. This capability is invaluable for incident investigation, root cause analysis, and gathering evidence for legal or compliance purposes.

- **Endpoint Remediation:** FortiEDR's EDR response facilitates endpoint remediation by automating the process of removing malicious artifacts and restoring compromised systems to a secure state. It streamlines the remediation workflow, saving time and effort for security teams while ensuring a thorough and consistent approach.
- **Threat Intelligence Integration:** A Fully Managed FortiEDR solution with EDR response leverages threat intelligence feeds to enhance its detection capabilities. By integrating with threat intelligence platforms and leveraging up-to-date threat intelligence, we can identify and respond to emerging threats faster, ensuring proactive protection against the latest attack techniques.
- **Centralized Management and Reporting:** With a Fully Managed FortiEDR solution, EDR response operations can be centrally managed. Administrators and our SOC team can oversee and control endpoint security measures from a unified dashboard, allowing for streamlined management and reporting across the state. This centralized approach simplifies administration, monitoring, and compliance reporting.
- **Continuous Monitoring and Protection:** FortiEDR's EDR response capabilities provide continuous monitoring and protection for endpoints. It monitors endpoint activities in real-time, detecting threats and suspicious behaviors promptly. This proactive monitoring ensures a high level of security against evolving threats, minimizing the risk of successful attacks.
- **Compliance and Audit Readiness:** A Fully Managed FortiEDR solution with EDR response helps organizations meet compliance requirements and maintain audit readiness. It offers robust endpoint security measures, comprehensive incident response capabilities, and reporting, enabling organizations to demonstrate their adherence to regulations and security best practices.

## Achieving the 99.999% Uptime

FortiEDR maintained an uptime of 99.999% in 2020-2021. While in 2022, the uptime dipped slightly to 99.99% but still maintains an impressive track record! In order to achieve 99.999% we have datacenters in multiple, geographically dispersed U.S. locations hosting multiple redundant and load balanced copies of FortiEDR. Monitored by our U.S. based SOC (Security Operations Center).

FortiEDR uses a variety of techniques to maintain it's high uptime, including:

- **Redundancy:** FortiEDR is deployed in a redundant configuration, with multiple appliances providing coverage for each endpoint in multiple datacenters. This helps to ensure that there is always an appliance available to protect endpoints, even if one appliance fails.
- **Load balancing:** FortiEDR is deployed in a load-balanced configuration, with multiple appliances sharing the workload of protecting endpoints. This helps to improve performance and can also help to prevent outages if one appliance fails.

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution





- Failover: FortiEDR is configured to automatically fail over to a backup appliance or datacenter if the primary appliance or datacenter becomes unavailable. This helps to ensure that endpoint protection is always available, even if there is an outage.

## Optional Added Services

### On-Site Training

On-site Training priced at a one-time \$6,000 1-day session.

- Details
  - Tailored Training Experience: On-site training allows organizations to customize the training program to meet their specific needs. Training providers can work closely with the organization to understand their goals, challenges, and desired outcomes, and design a curriculum accordingly.
  - In-person Interaction: With on-site training, participants have direct access to instructors who can provide real-time guidance, answer questions, and facilitate discussions. This interactive environment promotes engagement and fosters a deeper understanding of the subject matter.
  - Practical Application: On-site training incorporates practical exercises and simulations that allow participants to apply their knowledge in real-world scenarios. This hands-on approach enhances the learning experience and helps participants gain practical skills that can be immediately implemented in their work environment.
  - Team Building and Collaboration: On-site training brings employees together in a shared learning environment. It encourages collaboration, teamwork, and the exchange of ideas and experiences among participants. This can foster a sense of camaraderie and strengthen working relationships within the organization.
  - Focus and Concentration: On-site training provides a dedicated learning environment, free from distractions commonly found in the workplace. Participants can fully immerse themselves in the training material, ensuring maximum focus and concentration.
  - Contextualized Examples: On-site training can be customized to include examples relevant to the organization's industry, challenges, and specific use cases. This helps participants relate the training material to their own work environment and enhances the applicability of the knowledge gained.
  - Flexibility and Adaptability: On-site training can be scheduled at a time that is convenient for the organization, taking into account operational requirements and employee



availability. The training provider can adapt the program based on the participants' skill levels and adjust the pace to ensure effective learning.

- Personalized Support: On-site training offers the opportunity for personalized support and one-on-one interactions with instructors. Participants can receive individualized guidance, address specific questions or concerns, and receive immediate feedback, enhancing their learning experience.
- Cost-Effective for Larger Groups: On-site training can be cost-effective for organizations with a larger number of participants. Instead of sending employees to external training programs individually, the organization can leverage economies of scale by hosting the training on-site for a larger group.

## Managed & Monitored FortiSIEM

Pricing \$444.36/Device/Year

- Details

- Cloud-Based FortiSIEM Deployment: PCS sets up and manages the cloud infrastructure hosting FortiSIEM, relieving clients of the burden of infrastructure maintenance and management.
- Security Event Monitoring: PCS conducts continuous monitoring of clients' network, systems, and applications using FortiSIEM. They analyze security events, logs, and network flows to detect potential threats and anomalies.
- Incident Detection and Response: PCS leverages FortiSIEM to detect and respond to security incidents promptly. Their security analysts analyze events, investigate alerts, and initiate appropriate response alerts to help minimize the impact of security breaches.
- Threat Intelligence Integration: PCS integrates external threat intelligence feeds with FortiSIEM, enabling clients to benefit from up-to-date information on emerging threats, known attack vectors, and malicious actors. This integration enhances threat detection capabilities.
- Incident Detection and Alerting: PCS identifies security incidents from detection to alerting. They follow predefined alert response processes, provide emergency alerting, and escalate critical alerts to appropriate teams or individuals within the client organization.
- Compliance Monitoring and Reporting: PCS helps clients monitor compliance with industry regulations and standards. They can help configure FortiSIEM to generate compliance reports, track adherence to security policies, and support regulatory audits.

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



- Customizable Dashboards and Reporting: PCS creates customized dashboards and reports within FortiSIEM to provide clients with real-time visibility into their security posture. These dashboards and reports can be tailored to meet clients' specific requirements and provide meaningful insights.
- Log Management and Analysis: PCS manages log data collection, normalization, and analysis using FortiSIEM. They monitor logs from various sources, troubleshoot logging issues, and identify security incidents, all while ensuring efficient log management.
- Vulnerability Notifications: Using FortiSIEM, PCS notifies clients about vulnerabilities seen within their organization.
- Integration with Security Tools: PCS integrates FortiSIEM with clients' existing security tools, such as firewalls, antivirus solutions, and intrusion detection systems. This integration centralizes security information, streamlines workflows, and enhances overall security operations.
- Managed SIEM Service: PCS offers managed SIEM services, utilizing FortiSIEM as the core platform. They oversee the day-to-day operation of FortiSIEM, ensuring its performance, availability, and effectiveness in meeting clients' security monitoring needs.
- Security Consultation and Advisory Services: PCS provides security consultation and advisory services to clients, leveraging their expertise in FortiSIEM and broader security practices. They offer quarterly meetings to suggest recommendations, best practices, and guidance to enhance clients' security posture.

## Forensics and Remediation Services

Pricing \$210/hour

PCS offers a Cyber Forensics and Remediation Service that can help organizations to investigate and respond to cyber incidents. The service includes the following:

- Incident response: PCS will work with the organization to assess the incident and develop a response plan. This may include steps such as containment, eradication, and recovery.
- Forensic analysis: PCS will conduct a forensic analysis of the affected systems to gather evidence of the incident. This evidence can be used to identify the attacker, understand the attack vector, and prevent future attacks.
- Remediation: PCS will work with the organization to implement security controls to prevent future attacks. This may include steps such as patching vulnerabilities, implementing security policies, and training employees on security best practices.

PCS' Cyber Forensics and Remediation Service can help organizations to:

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



- Minimize the impact of a cyber incident: PCS can help organizations to contain and eradicate the attack, and to recover from the incident as quickly as possible.
- Gather evidence: PCS can gather evidence of the attack, which can be used to identify the attacker and prevent future attacks.
- Implement security controls: PCS can help organizations to implement security controls to prevent future attacks.

Additional products or services offered to state agencies at a minimum of a 3% discount.

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.

PC Solutions & Integration, Inc.

Vendor Name

*Robert S. Boush*

Signature

65-0798706

FEIN

Robert Boush

Signatory Printed Name

5.16.23

Date



## Attachment B

### ATTACHMENT B CONTACT INFORMATION SHEET

#### I. Contact Instructions

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

#### II. Contact Information

	Contact for Quoting Purposes	Contact for the ATC and PO (if awarded)
<b>Name:</b>	Natasha Rolle	David Rudnick
<b>Title:</b>	Inside Sales Manager	VP of Sales
<b>Address (Line 1):</b>	4937 SW 75th Avenue	4937 SW 75th Avenue
<b>Address (Line 2):</b>		
<b>City, State, Zip Code</b>	Miami, FL 33155	Miami, FL 33155
<b>Telephone (Office):</b>	305-667-0633	305-667-0633
<b>Telephone (Mobile):</b>	786-391-4744	786-391-4748
<b>Email:</b>	sales@pcsusa.net	david@pcsusa.net



# Non-Disclosure Agreement

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

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

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

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

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

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

### 1. Definitions.

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



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

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

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



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

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

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

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





**9. Contractual Remedies.** Recipient acknowledges that a breach of this Agreement, including disclosure of any of the Confidential Information, will cause irreparable injury to the Department or the Customer and will entitle the Department or the Customer, if applicable, to liquidated damages commensurate with the Department's or the Customer's internal staffing and administrative costs associated with addressing the breach. This will not preclude the Department or the Customer from recovering other damages it may suffer as a result of such a violation or seeking other legal remedies that may be available during or after the Agreement term, including obtaining injunctive relief against the breach or threatened breach of these Agreement terms.

**10. Data Destruction.** Prior to the termination of this Agreement, Recipient shall assist the Department or the applicable Customer in exporting and extracting or destroying, at the Department's or the applicable Customer's direction, all information obtained from the Department or the applicable Customer by Recipient or created for the Department or the applicable Customer by Recipient pursuant to this Agreement at no cost, in a format acceptable to the Department or the applicable Customer without the need to purchase additional services and/or commodities. Additionally, when the Agreement is terminated, Recipient shall transfer to the Department, or the Customer as applicable, all such information in all its forms from the Department or the applicable Customer and shall destroy duplicate records in accordance with section 501.171(8), F.S., and, if applicable, section 119.0701, F.S. This obligation to transfer and destroy information survives the term of this Agreement.

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

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

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

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



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

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

**FLORIDA DEPARTMENT OF MANAGEMENT SERVICES**

By: \_\_\_\_\_  
Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Date: \_\_\_\_\_

By: David H. Rudnick  
Name: David Rudnick  
Title: Vice President  
Date: 5.16.23

## Partnerships (Subcontractors)

The below will identify all subcontractors the vendors will utilize to provide the services required by this RFQ and what services each subcontractor will provide.

### PCS and SkyHelm Partnership

Skyhelm is one of PCS’ strategic partners. This partnership between PCS and SkyHelm was formed to deliver specialized security services to bring the strengths of the two companies together and be able to service our clients better. SkyHelm’s mission is to protect America’s critical infrastructure technology. Our combined teams are passionate about solving complex technology challenges by focusing on the outcomes our customers care about and by applying our extensive industry-specific experience. Together with your team, we design, implement, and manage complete cybersecurity and infrastructure technology solutions for organizations like municipalities, public safety, utilities, and more.



## Services

Both PCS and SKyHelm are US based cybersecurity companies that employ local technology talent with a 24/7/365 state-of-the-art Security Operations Center (SkySOC) in Oklahoma City, Oklahoma. Our US-Based team of trained and certified cybersecurity professionals have the experience and talent to improve your organization's cybersecurity posture.

Our team has an intimate knowledge of critical infrastructure cybersecurity needs including compliance requirements, best practices and funding. Additionally, our teams have worked with state organizations for over a decade and are knowledgeable in your particular needs.

### **Technology Consulting**

- Network Reliability
- Networking Segmentation
- Server Infrastructure
- Technology Deployment Strategies
- Software Deployments and Integrations
- Cloud Migrations
- Custom Application Development
- SD-WAN (Software Defined Wide Area Network)
- Edge Device Communications
- Wireless Networking
- Fiber Deployments (Both Private and ISP Experience)

### **ICS Systems Consulting**

- OT Control Systems
- OT Databases
- Database Development
- Custom Application Development
- Operation Communications
- Dispatching Control Centers
- Smart Grid
- High Speed Relaying
- Radio Communications
- Metering Technologies



### **CyberSecurity Consulting**

- Managed Cyber Security
- Managed Firewall
- Penetration Testing
- Security Reviews
- Policy Reviews/Development
- Endpoint Management
- Network Security
- Data Loss Prevention
- Security Information and Event Management (SIEM)
- Multi-factor Authentication Migration
- Network Intrusion Prevention
- Security Policy Reviews/Recommendations
- Tailored Employee Security Awareness Training
- Compliance Management

### **24/7 Monitored NOC and SOC**

We have a 24/7/365 NOC and SOC based out of Oklahoma with backup facilities in Colorado and Texas. We have skilled systems and network security professionals in place to monitor your infrastructure, along with several other organizations. Our SOC employs sandboxing technology to detect threats before they're known, we use AI-driven security tools that can block advanced attacks, but most importantly we have a dedicated team with an understanding of how your network traffic should look. The security and reputation of your organization is paramount, and we want to partner with you to ensure it remains intact. Choose us to receive the best in incident detection, investigation, vigilance, and response.



# **PCS Experience & Related Project History**



SIMPLIFY WITH TECHNOLOGY

# SHAPING EDUCATION THROUGH TECHNOLOGY

*PCS has worked together with numerous private and public K-12 and Higher Education institutions with one clear goal in mind: To leverage the power of technology to create connected and collaborative environments for students, teachers, and staff. We want to bring the transformative power of technology to every classroom and offer the experience, expertise, and resources to help you design, implement, and maintain your IT investments.*

## EXPERIENCE

### FLORIDA SCHOOL DISTRICTS

- Bay County
- Calhoun County
- Gadsden County
- Hardee County
- Hendry County
- Jackson County
- Martin County
- Okaloosa County
- Palm Beach County
- Santa Rosa County
- Wakulla County
- Walton County

### GEORGIA SCHOOL DISTRICTS

- Banks County
- Bartow County
- Beaufort County
- Columbia County
- Coweta County
- Dade County
- Dodge County
- Jefferson City
- Madison County
- McDuffie County
- Morgan County
- Newton County

### UNIVERSITIES & COLLEGES

- Clayton State University
- Florida Gulf Coast
- Florida International University
- Hillsborough Community College
- Mercer University
- Rollins College
- St. Petersburg Community College
- St. Thomas University
- Tallahassee Community College
- University of Central FL
- University of Miami
- University of West Georgia



SIMPLIFY WITH TECHNOLOGY

## WHAT OUR CUSTOMERS ARE SAYING

“ PCS has been the choice vendor on several projects with the Columbia County School District. Although new to Georgia, PCS has developed a strong following in other states due to a strong focus on the K-12 vertical. Our district has been pleasantly pleased with the level of customer support and care PCS has delivered to the Columbia County School District. In addition, to both presale and post-sale support, the level of technical engineering brought to the Columbia County School District has both saved the district money while improving the IT infrastructure for our students.”

**-James Van Meter**

CTO, COLUMBIA COUNTY SCHOOLS

“ PCS has provided St. Petersburg College with excellent service and flexibility. They understand the education market and the challenges we face to continuously improve our technology infrastructure and services while living within our funding and procurement procedures.”

**-David Creamer**

CTO & CISO, St. Petersburg College

## LOCATIONS

*PCS has strategic local offices throughout the SE United States.*

- Miami, FL (Headquarters)
- Tampa, FL
- Tallahassee, FL
- Atlanta, GA
- Dallas, TX
- Nashville, TN





## A Few of our Satisfied Networking Clients

### **Walton County School District**

Contact: Janie Griffith  
Address: 145 Park Ave Defuniak Springs, FL 32433  
Email: [griffithkj@walton.k12.fl.us](mailto:griffithkj@walton.k12.fl.us)  
Telephone Number: 850-892-1100

### **Bay County School District**

Contact: Les Hooe  
Address: 1311 Balboa Avenue Panama City, FL 32401  
Email: [hooeld@bay.k12.fl.us](mailto:hooeld@bay.k12.fl.us)  
Telephone Number: 850-767-4206

### **Palm Beach School District**

Contact: Kevin Ogonowski  
Address: 3300 Forest Hill Blvd., West Palm Beach, FL 33406  
Email: [kevin.ogonowski@palmbeachschools.org](mailto:kevin.ogonowski@palmbeachschools.org)  
Telephone Number: 561-434-8920

### **Okaloosa County School District**

Contact: Barry Boutwell  
Address: 120 Lowery Place SE Fort Walton Beach, FL 32548  
Email: [barry.boutwell@l-3com.com](mailto:barry.boutwell@l-3com.com)  
Telephone Number: 850-833-3163

### **Gadsden County School District**

Contact: John Thomas  
Address: 35 Martin Luther King Jr. Blvd. Quincy, FL 32351  
Email: [thomasj@gcpsmail.com](mailto:thomasj@gcpsmail.com)  
Telephone Number: 850-627-9651

### **Washington County School District**

Contact: Sandra Coppedge  
Address: 652 3<sup>rd</sup> Street Chipley, FL 32428  
Email: [Sandra.coppedge@washington.k12.fl.us](mailto:Sandra.coppedge@washington.k12.fl.us)  
Telephone Number: 850-638-6222

### **Client: University of Miami**

Contact: Kenrick Thomas  
Address: 1320 S. Dixie Highway, Coral Gables, FL 33124  
Email: [kenrick@miami.edu](mailto:kenrick@miami.edu)  
Telephone Number:





**Client: University of Central Florida**

Contact: Lou Garcia

Address: 4000 Central Florida Blvd., Orlando, FL 32816

Email: [Lou.Garcia@ucf.edu](mailto:Lou.Garcia@ucf.edu)

Telephone Number: 407-823-4945

Brief Description: University of Central Florida is the 2<sup>nd</sup> largest University in the United States. UCF relies on PCS to supply and support their Extreme Networks equipment.

**Client: Orlando Magic**

Contact: Joel Massey

Address: 8701 Maitland Summit Boulevard, Orlando, FL 32810

Email: [jmasse@orlandomagic.com](mailto:jmasse@orlandomagic.com)

Telephone Number:

Brief Description: The Orlando Magic have relied on PCS to support their network for multiple years.

**Client: Valencia Community College**

Contact: Kevin Moll

Address: 1800 South Kirkman Road, Orlando, FL 32811

Email: [kmoll@valenciacollege.edu](mailto:kmoll@valenciacollege.edu)

Telephone Number:

Brief Description: Valencia Community College has a large amount of equipment from PCS installed within 4 campuses.

**Client: Arquitectonica**

Contact: Jorge Jimenez

Address: 2900 Oak Avenue, Miami, FL 33133

Email: [jjimenez@arquitectonica.com](mailto:jjimenez@arquitectonica.com)

Telephone Number: 305-372-1812

Brief Description: Arquitectonica is one of the world's largest architecture firms with operations in 4 continents. PC Solutions has designed, deployed, and managed their worldwide network.

**Client: Florida Gulf Coast University**

Contact: Sven Hagues

Address: 10501 FGCU Boulevard, Fort Myers, FL 33965

Email: [shagues@fgcu.edu](mailto:shagues@fgcu.edu)

**Client: AO Smith**

Contact: Chris Stinson

Address: 106 Adkisson Street Ashland City, TN 37015

Email: [cstinson@hotwater.com](mailto:cstinson@hotwater.com)

Telephone Number: 615-792-6256

Brief Description: While not a household name, AO manufactures most of the hot water heaters sold in the United States. Their size, global reach and the harsh environment of their manufacture plants makes them one of our more unique clients. One of their manufacturing plants is over 1 mile long. PCS now supplies and supports their wired and wireless infrastructures.

## PCS - Relevant Project Experience

### City of Tallahassee

Design and implementation of new network infrastructure. This project was to replace a single flat network. Project encompassed the implementation of an enterprise DHCP/DNS system, routing to each IDF, multiple redundant paths to resources, enterprise wide device and user authentication, enterprise wireless implementation, implementation of policy enforced at the edge, and enterprise management of the entire environment. Project was accomplished in multiple phases;

1. Network audit
2. Identify requirements and limitations
3. Preliminary design
4. RFP process and procurement
5. Staging and testing
6. Implementation planning and scheduling
7. Implementation execution

#### - Phase 1: Audit

- Inspect each location and all associated IDFs
  - Determine existing network capability and utilization
  - Determine physical infrastructure status
  - Determine need and/or use of wireless
- Evaluate the physical WAN capability
  - Owned fiber types and distances
  - Leased fiber types and distances
  - T-1 implementation
  - DSL implementation
- Document the existing network design, hardware, and connectivity.
- Evaluate existing layer 3 logical segmentation, address assignment methodology, and document
- Evaluate existing DNS and domain implementation and document
- Evaluate type and number of devices utilizing the network and document
- Evaluate type and number of users and their resource requirements and document
- Evaluate existing internet connectivity, DMZ configuration, firewall implementation, and
- Evaluate security requirements for;
  - CJIS compliance: Public Safety
  - NERC/FERC Compliance: Public Utilities
  - FAA Compliance: Airport
  - PKI Compliance
  - Sarbanes-Oxley Compliance
  - HIPPA Compliance

- **Phase 2: Determine Requirements and Limitations**
  - Hold numerous meetings with stakeholders, IT management and IT divisions to determine and state the desired results of the project.
    - Review the results of the audit
      - State the current capabilities, limitations and pitfalls
      - State proposed changes to the design and methodology of the infrastructure.
      - Explain how the proposed changes will benefit the organization
    - Determine all requirements for use, access, and security as it pertains to network usage.
    - Identify all current issues, perceived and real, to be addressed by the network.
    - Identify new features and functionality wanted (not a requirement) as part of the re-design.
    - Identify possible and known future requirements for the network.
    - Identify budgetary requirements
      - Limits and constraints
      - Capital (purchase) versus recurring (lease)
      - Terms; single year, multiple year
    - Identify timeframes and associated limitations
    - Identify outage availability and limitations
    - Identify resource requirements and availability
    - Deliver high level proposal for redesign and obtain buy in to move forward.
  
- **Phase 3: Preliminary Design**
  - Utilize the information obtained in phase one and two start the design process
    - Requirements
      - Migrate from a flat/bridged network to routed network
      - Implementation of a new IP addressing schema
      - Implementation of DHCP
      - Migration of DNS from Domain Controllers to enterprise systems
      - Implementation of user and device authentication
        - Domain users and computers to utilize 802.1X for authentication
        - Non-domain devices to be authenticated by MAC address/Vendor-OUI
        - Guest will utilize a sponsorship methodology to gain access
      - Implementation of edge enforced policy to control user and device usage of the network and its resources
        - Domain authenticated users to have different policies based on resource requirements

- Domain computers to only access remediation systems
    - Non-domain devices to have different device type, use and resource requirements
    - No user/device to user/device communications will be allowed
    - No user/device can provide network services or utilize network management protocols (server farm omitted)
    - Guest will only have access to the internet
  - Unified management system for network configuration and firmware management, inventory/asset management, logging and alerting, user and device authentication, and policy management and enforcement. Wireless system management preferred.
  - Unified management system for DNS and DHCP system.
  - Addition of Power over Ethernet capabilities (PoE and PoE+)
  - Standardized models based on IDF capacity requirements
  - Sparring plan to accomplish four-hour hardware replacement by internal staff for critical locations, next day replacement for all other locations.
  - Ability to upgrade uplink capabilities in the backbone and to IDFs without a forklift upgrade.
  - Design with a 20% growth potential and 10-year lifespan
  - Design with N+1 redundancy for core network functions
  - Re-design of Server Farm to compensate for high East-West and backup utilization.
  - Enhanced security posture for the entire enterprise
  - Enterprise wireless with ability for secure, segregated Guest access.
- Backbone (per location)
    - Develop routing design and IP schema
    - Document port counts and speed capability requirements
    - Document transceiver requirements and counts
    - Document power requirements
    - Document physical space requirements/limitations
    - Documents new patch cord, fiber and copper, counts
    - Generate a generic Build-of-Materials for the Backbone
    - Diagram the backbone design and start overall network design diagram.
  - IDF requirements
    - Determine if this is a routed IDF
      - If Yes,
        - Part of a router spur or loop
          - Identify uplink neighbor
          - Identify downlink neighbor
        - Develop routing configuration
      - Develop IP addressing per IDF and naming convention, including physical mailing address, floor, room ID, etc.
    - Document IDF port count requirement to determines switch type/size
      - 18 or less ports equate to a 24-port switch

- 24 to 36 ports equate to a 48-port switch
    - Greater than 36 ports equate to a chassis capable of up to 144 ports
  - Document WAN connectivity
    - Fiber (type and distance)
    - T-1 (additional T-1 router required, no transceiver required)
    - DSL (no transceiver required)
  - Document uplink counts, speed capability, and transceiver requirement
  - Document power requirements
  - Document physical space requirements/limitations
  - Documents new patch cord, fiber and copper, counts
  - Generate a generic Build-of-Materials for the each IDF
  - Diagram each standalone IDF design and add to overall network diagram.
- Enterprise wireless requirements
  - Document capacity and growth requirements
  - Document redundancy requirements, as well as, N+1 requirement
  - Document Microsoft Domain integration requirements
  - Documents network management integration requirements
  - Document security capability requirements
  - Documents logging and alerting requirements
  - Generate a generic Build-of-Materials for the wireless implementation
  - Diagram standalone wireless system design and add to overall network diagram
- DNS/DHCP system requirements
  - Document capacity and growth requirements
  - Document redundancy requirements, as well as, N+1 requirement
  - Determine the locations for physical dispersion of the system and number of nodes
  - Document Microsoft Domain integration requirements
  - Document unified management with logging and alerting requirements
  - Generate a generic Build-of-Materials for the DNS/DHCP system implementation
  - Diagram standalone DNS/DHCP design and add to overall network design diagram
- Management, Authentication, and Policy enforcement system
  - Document capacity, function, and growth requirements
  - Documents redundancy requirements
  - Determine the locations for physical dispersion of the system and number of nodes
  - Document authentication type requirements, as well as, N+1 requirement
  - Document Microsoft Domain integration requirements
  - Documents Policy development, management, and enforcement requirements
  - Documents logging and alerting requirements
  - Generate a generic Build-of-Materials for the system implementation
  - Diagram the system and add to overall network design diagram

- **Phase 4: RFP process and procurement**

- Create RFP based on preliminary design, diagrams and Build-of-Materials developed in phases one through three.
- Develop script for Proof of Concept presentations.
- Evaluate RFP responses and determine vendor short list.
- Short listed vendors present a scripted Proof of Concept for evaluation.
- Choose solution.
- Procure equipment through procurement process.
  - Arrange for all equipment to be shipped to storage/staging facility
- Order any new fiber and copper patch cables
  - Requirements were determined during phase three.
- Order any wiring modification utilizing existing wiring contractor.
  - Physical infrastructure requirements were determined during phase one.

- **Phase 5: Staging and Testing**

- Inventory all deliveries against invoice
  - Document all serial numbers
  - Build all switches and routers, power the device, and test for DOA failures
  - Identify any DOA hardware and RMA immediately.
  - Apply property tags as required.
- Build the backbone, configure, and test routing, redundancy, failure recovery
  - Upgrade firmware as needed to a current supported revision (vendor recommendation)
  - Configure routers based on configurations and documentation developed in phase three.
  - Test routing, redundancy, alternate paths and failure recovery.
  - Modify configurations as needed and update all documentation
  - Re-test as needed, modify configurations, and update documentation until no failures.
  - Label the device based on naming convention.
  - Connect to existing network to access resources
- Build IDF switches, configure, and test
  - Upgrade firmware as needed to a current supported revision (vendor recommendation)
  - Configure switches based on configurations and documentation developed in phase three.
  - Test connectivity, access to resources via the backbone.
  - Modify configurations as needed and update all documentation
  - Re-test as needed, modify configurations, and update documentation until no failures.

- Label the device based on naming convention.
- Build the DNS/DHCP system, configure, and test
  - Upgrade firmware as needed to a current supported revision (vendor recommendation)
  - Integrate with the domain
  - Configure and test DNS
    - Migrate any records from the domain DNS to new DNS
    - Check that service records are being received from the domain
    - Check resolution within the existing network and to the Internet
  - Configure and test DHCP in the staging environment
    - Test dynamic address assignment
      - Check mask, gateway, other information delivered via DHCP
      - Check that Host records are being dynamically created in DNS
    - Test static address assignment
      - Check that Host records are being dynamically created in DNS
    - Test that devices with dynamic or static assigned addresses can be reached via host name (DNS resolution)
  - Add all new scopes to DNS/DHCP for each IDF
  - Test DNS and DHCP on each IDF switch.
  - Re-test as needed, modify configurations, and update documentation until no failures.
- Build the Authentication and Policy system
  - Upgrade firmware as needed to a current supported revision (vendor recommendation)
  - Integrate with the domain
  - Create two policies
    - Authentication = accept, Policy = GOOD (allow all)
    - Authentication = reject, Policy = BAD (deny all)
    - Configure the policies to the IDF switches (pushed from management system)
  - Configure authentication
    - Configure IDF switches for RADIUS configuration (pushed from management system)
    - Domain Authentication
      - Configure LDAP for authentication of domain users and devices against the domain
      - Test multiple device types and multiple users
      - Test and re-test as needed, modify configurations, and update documentation until no failures.
    - MAC/Vendor-OUI Authentication
      - Configure MAC/Vendor-OUI authentication
      - Test and re-test as needed, modify configurations, and update documentation until no failures.

- Document the configuration changes for domain devices for the utilization of 802.1X is required.
  - Configure the complete policy implementation utilizing the documentation developed in phases one through three.
    - Configure the policies to the IDF switches (pushed from management system)
    - Test each policy and re-test as needed, modify configurations, and update documentation until no failures.
  - Finalize implementation of management systems
    - Test visibility
      - All new switches and routers
      - All new authentication and policy enforcement nodes
      - All new DNS/DHCP nodes
      - End-Users (authentication, DNS resolution, MAC & IP addressing)
    - Test logging and alerting
      - Local
      - SMTP
      - Other
    - Confirm all new devices are represented in the system
    - Confirm all new devices are scheduled for automatic backup
      - Perform a one-time backup of all configurations once staging is complete and all configuration are set
    - Verify that all new IDF devices have the correct complete policy configuration.
    - Verify that all new IDF devices have the correct complete RADIUS configuration.
  - Finalize all documentation for this phase
    - Configuration files
    - Inventory – Property Tags
    - Diagrams
- **Phase 6: Implementation planning and scheduling**
  - Develop an implementation plan
    - Backbone implementation
      - Rack and stack new equipment co-located with existing network at each of the six locations
      - Power up equipment and connect WAN connections
      - Test all connectivity and routing functions
      - Connect core backbone router to existing core
      - Test new to old network connectivity



- Confirm network documentation represents physical connectivity accurately
- Backout: disconnect from existing core if problems occur.
- DNS/DHCP implementation
  - Rack and stack all nodes at six backbone router locations
  - Power up equipment and connect to backbone router
  - Test all connectivity
  - Test DNS functionality
  - Test DHCP functionality
  - Confirm network documentation represents physical connectivity accurately
  - Backout: disconnect from existing core if problems occur.
- Authentication implementation
  - Rack and stack all nodes at six backbone router locations
  - Power up equipment and connect to backbone router
  - Test all connectivity
  - Test authentication and policy enforcement functionality
  - Confirm network documentation represents physical connectivity accurately
  - Backout: disconnect from existing core if problems occur.
- IDF Switch implementation (repeat for each IDF)
  - Rack and stack new switch co-located with existing equipment if space is available
    - If space is not available, old equipment will be de-installed
  - Power up switch
  - Connect to backbone
  - Confirm backbone connectivity
  - Confirm authentication and policy enforcement with test user/device
  - Confirm access to network resources and internet
  - Confirm network documentation represents physical connectivity accurately
  - Do not migrate users if any of the above is not operational.
  - Cut over existing devices to new switch
    - Utilize implementation notes for end device reconfiguration
    - Reconfigure domain computers if required
      - Clear static IP and configure DHCP
      - Configure 802.1x supplicant on computer
      - Confirm authentication, DHCP and access functionality
      - Document changes made to device configuration
    - Reconfigure non-domain equipment if required
      - Re-configure static IP address for new scope
      - Confirm authentication and access functionality
      - Document changes made to device configuration

- Backout:
  - migrate users back to original switch if still installed
  - re-install original switch and migrate users back
  - undo and changes made to devices
  - re-test device access to network and functionality
- Scheduling
  - Backbone implementation
    - Time and resources required
      - sixteen man-hours per site
      - six backbone sites
      - Network staff only
    - Outage Requirements
      - Racking stacking: no impact
      - Power up and connecting WAN: no impact
      - Cross connect to existing backbone: possible impact
        - Schedule for Sunday after backup routine is complete.
  - DNS/DHCP implementation
    - Time and resources required
      - Two man-hours per site
      - Six backbone locations
      - Rack and stack can be completed during backbone rack and stack
      - Network staff only
    - Outage Requirements
      - Racking stacking: no impact
      - Power up and connecting to backbone: possible impact
        - Schedule after backbone cross connect is complete and running for one week
        - Schedule for Sunday after backup routine is complete
  - Authentication implementation
    - Time and resources required
      - Two man-hours per site
      - Six backbone locations
      - Rack and stack can be completed during backbone rack and stack
      - Network staff only
    - Outage Requirements
      - Racking stacking: no impact
      - Power up and connecting backbone: possible impact
        - Schedule after backbone cross connect and DNS/DHCP implementation are complete and running for one week
        - Schedule for Sunday after backup routine is complete
  - IDF: Equipment Rack and Stack
    - Time and resources required

- Variable depending on IDF (Appendix A)
      - Rack and stack can be completed during normal business hours in locations where space is available to co-locate with existing equipment (Appendix A)
      - Network staff only
    - Outage Requirements
      - Rack and stack can be completed during normal business hours in locations where space is available to co-locate with existing equipment (Appendix A): no impact
      - Locations where existing equipment must be de-installed before new equipment is implemented: complete outage, will be completed during schedule IDF cutover
  - IDF: Cutover
    - Time required
      - Variable depending on IDF (Appendix B)
      - Rack and stack can be completed during normal business hours in locations where space is available to co-locate with existing equipment (Appendix B)
      - Network, Server, PC staff
    - Outage Requirements
      - Complete outage for all devices terminated in the specific IDF
  - Wireless Implementation
    - Time and resources required
      - This will be done as time allows after all IDFs, Users and Devices are operational.
      - Network staff only
- **Phase 7: Implementation execution**
  - Implementation will follow the schedule set forth in the Gantt chart (Appendix C)
  - All configuration documentation in Appendix D will be used and updated, as needed, through completion of the project.
  - All diagrams in Appendix E will be used and updated, as needed, until completion of the project.
  - All communication to end users concerning scheduled outages will be communicated by the Project Manager for this project.
  - All issue reporting will follow normal procedure, except during a cut over, in which case the Network Administrator will be informed.

## PCS - Relevant Project Experience

### Florida Lottery

Design and implementation of the Florida Lottery's network upgrade. This project encompassed the replacement with upgraded equipment of all switches, router, wireless, and management systems state wide. The goal of the project is to upgrade to current equipment, upgrade physical infrastructure where required to support higher connection speeds, consolidate space and equipment where feasible, and implementation of newer protocols where applicable. There was no change to topology. The implementation was executed in multiple phases.

- Phase 1:
  - a. Determine replacement equipment requirements based on current capacity and future expansion considerations.
  - b. Determine to upgrade fiber to IDFs to support 10G uplink capabilities.
  - c. Determine new configurations for core, server farm, and internet connectivity to take advantage on newer protocols to enhance speed and redundancy.
  - d. Determine hardware requirements for all wireless, authentication, and management appliances, as well as new analytics appliance.
  - e. Determine new licensing requirements or license upgrade requirements for wireless, authentication, management, and analytics systems.
- Phase 2:
  - a. Inventory all new equipment against BOM and invoices.
  - b. Label and apply property tags.
  - c. Upgrade all firmware to latest support revision (per Vendor suggestion).
- Phase 3:
  - a. Stage new core equipment and test.
  - b. Stage new server farm equipment and test.
  - c. Stage new IDF equipment and test.
- Phase 4:
  - a. Install new core equipment, cross connect to existing core, and test
  - b. Install new server farm equipment, connect to new core, and test.
  - c. Install new IDF equipment in main facility IDFs, connect to new core via new fiber, and test.
- Phase 5:
  - a. Backup all existing wireless, authentication, and management systems in preparation for replacement.
  - b. Wireless System
    - i. Bring up new wireless appliances and load backup from existing system.
    - ii. Confirm configuration
    - iii. Disconnect existing appliances from network and connect new appliances.
    - iv. Confirm access point connectivity and visibility on the new appliances.
    - v. Confirm wireless operation.
  - c. Management System

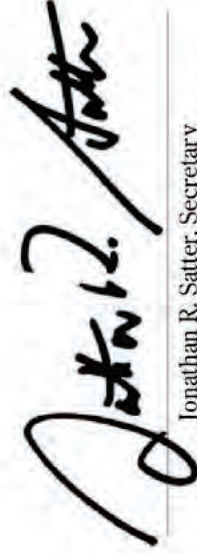
- i. Bring up new management appliance with new address
      - ii. Load backup configuration from existing system
      - iii. Upgrade system to current supported revision
      - iv. Upgrade and re-host licenses as needed
      - v. Add new network equipment to new management system
      - vi. Confirm operation of system and visibility of new network equipment.
    - d. Authentication System
      - i. Bring up new authentication appliances with new addresses
      - ii. Confirm visibility of new appliances by new management system
      - iii. Push configuration from new management system and confirm configuration.
      - iv. Add new equipment to the authentication system and confirm RADIUS configuration.
      - v. Test device and user authentication on new network IDF equipment.
- Phase 6: Cut Over to new Core and server farm equipment
  - a. Cut over to occur after hours.
  - b. Move Internet and WAN connections to new core.
  - c. Test connectivity from existing network to Internet and remote sites.
  - d. Test access to existing server farm and new server farm.
  - e. Migration of Servers to new farm to be completed as-time-allows by the Client.
- Phase 7: Cut Over users and devices to new IDFs in main facility
  - a. To be performed after hours, multiple IDFs, multiple cut over windows.
  - b. Testing of authentication and access has already been completed in phases four and five.
  - c. Migrate patch cables from existing equipment to new equipment.
  - d. Spot check computers, printers, and other equipment to confirm authentication and access to resources.
  - e. Original equipment will be removed after the new equipment has had time to burn in without issue. Timeframe is at the Clients discretion and will be accomplished by the Client.
  - f. Backout plan: revert patch cable connections to original equipment.
- Phase 8: Remote Site IDF cut over
  - a. Repeat phase seven for each remote site.
  - b. Client to schedule maintenance window for each location and communicate schedule.
  - c. Engineer will assist with the first three remote sites as OJT for the Client
- Phase 9: Removal of existing equipment and disposal
  - a. Client is responsible for the removal and storage of equipment
  - b. Client is responsible for the surplus of equipment per the Organization's policies and procedures.

State of Florida

Minority Business Certification

pc solutions & integration, inc.

Is certified under the provisions of  
287 and 295.187, Florida Statutes, for a period from:  
06/24/2021 to 06/24/2023



Jonathan R. Satter, Secretary  
Florida Department of Management Services



Office of Supplier Diversity  
4050 Esplanade Way, Suite 380  
Tallahassee, FL 32399  
850-487-0915  
www.dms.myflorida.com/osd



**SIMPLIFY WITH TECHNOLOGY**



**A LEADING IT  
SOLUTIONS PROVIDER**

[www.pcsusa.net](http://www.pcsusa.net)

# SIMPLIFY WITH TECHNOLOGY

## **OUR VISION** & MISSION

Our commitment is to be an expert advisor of hybrid IT solutions that give every customer, staff member, and audience a better experience. By providing scalable IT infrastructure, companies benefit from highly efficient and profitable IT investments that drive a measurable competitive advantage.



# A LITTLE ABOUT US



***Founded 22 years ago, PC Solutions & Integration (PCS) is the South Eastern United States premier integrator of IT services.***

When you work with PCS, you are working with a full-service provider. We are focused on supporting our clients throughout the project lifecycle, from consultation and design to implementation, optimization, and ongoing management. Our comprehensive portfolio provides one of the broadest and deepest solution offerings in the industry and is backed by a nationwide team of highly trained and certified technicians.

PC Solutions & Integration (PCS) is a leading IT services provider of collaboration and technology solutions for large and medium enterprises. We have spent decades building upon our technology offerings which span the core technology markets-collaboration, enterprise networking, data center, cloud, and security. We deliver these offerings across several delivery models including on premise, private, hybrid, and public clouds regardless of clients existing infrastructure.

## OUR PROFILE

---

*PCS offers innovative Premise and Cloud based best-of-breed products for Cyber Security, Desktop Computing, Networking, Data Center, Storage, Voice and Video.*

## WHAT WE DO

---

- ✓ **IT Health Checks**  
*Gain peace of mind knowing your system are performing optimally*
- ✓ **Proactive Maintenance**  
*We discover and then eradicate problems before they create downtime*
- ✓ **Enterprise Design & Scoping**  
*From consultation, to design, to implementation, to ongoing support, we're with you at every step.*

# OUR SERVICES

*Over the years, we have developed a proven track record of successes in Cyber Security, Storage, Voice Communications, Data Networks, Video, Wi-Fi, and UC Applications.*



## WIRELESS NETWORK INFRASTRUCTURE

PCS provides network auditing, design optimization, and maintenance to predict and respond to your growing network needs.



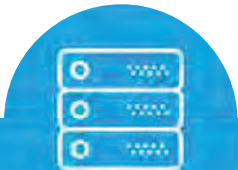
## CYBER SECURITY

The threat landscape is complex, but your security doesn't have to be. PCS can help you protect your networks, implement industry standards, follow best practices, and reduce attack surfaces.



## WIRED NETWORK INFRASTRUCTURE

Wired infrastructure is a crucial part of most organizations and has only grown in complexity. To manage that complexity, you need a team with a diverse skill set and a vendor-neutral approach.



## DATA CENTER/VIRTUALIZATION

The volume of data your business must manage has exploded. You need infrastructure that can capture, store, and archive massive amounts of data, while still keeping it readily accessible.



## PRO SERVICES

IT should support your core business, not overtake it. Do you need to offload mundane service tasks? Do you need full support and strategic planning for the entire IT function? No matter where you fall on that spectrum, PCS can help.



## UNIFIED COMMUNICATION

Unifying all of your businesses communication tools amplifies their power to transform your business through greater efficiency, better customer service, and stronger connections.

# TECHNOLOGY PARTNERS

*We are firm believers that when it comes to technology one size or partner does not fit all. That is why we work with more than 200 of the world's leading best of breed hardware, software, and application development companies so that we can bring you the right solution for your unique situation.*



# OUR MARKET



**CORPORATE HQ**  
MIAMI | FLORIDA

**4937 SW 75 Avenue**  
**Miami, FL 33155**

**T:** 305.667.0633  
**F:** 305.667.0618

**TAMPA,  
FLORIDA**

**4907 North Florida Avenue**  
**Tampa, FL 33603**

**T:** 813.703.8258

**TALLAHASSEE,  
FLORIDA**

**113 South Monroe Street**  
**Tallahassee, FL 32301**

**T:** 850.270.6930

**BIRMINGHAM,  
ALABAMA**

**One Perimeter Park South,**  
**STE 100N**  
**Birmingham, AL 35243**

**T:** 205.449.1168

**NASHVILLE,  
TENNESSEE**

**3200 West End Avenue**  
**Suite 500**  
**PMB 5312**  
**Nashville, TN 37203**

**T:** 615.866.0954

**ATLANTA,  
GEORGIA**

**1201 Peachtree Street 400**  
**Colony Square, STE 200**  
**Atlanta, GA 30361**

**T:** 470.440.9265



## Attachment A

### ATTACHMENT A PRICE SHEET

#### I. Alternate Contract Source (ACS)

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

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

#### II. Pricing Instructions

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

#### III. Pricing

Initial Term Pricing (Years 1-3)		
Item No.	Description	Rate Per Device
1	<p><b>Initial Software Year</b> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> <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>	\$ <b><u>\$56.99</u></b>
2	<p><b>Subsequent Software Year</b> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> <li>• <b>ongoing training</b></li> <li>• integration maintenance</li> <li>• support services</li> </ul>	\$ <b><u>\$53.11</u></b>

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



Optional Renewal Term Pricing (Years 4-6)		
Item No.	Description	Rate Per Device
1	<p><b>Initial Software Year</b> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> <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>	\$ <u><b>\$53.11</b></u>
2	<p><b>Subsequent Software Year</b> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> <li>• <b>ongoing training</b></li> <li>• integration maintenance</li> <li>• support services</li> </ul>	\$ <u><b>\$53.11</b></u>

#### 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
FC	1-10-FEDR1-377-01-12	FortiEDR-25 FortiEDR Discover, Protect	\$2,550.00	\$2,167.50
	FP-10-MDR-FRNSCS	FortiEDR Managed Detect and Respond	\$400.00	\$388.00

Item No. 2 – ACS Pricing Breakdown (without implementation)				
	ACS SKU Number	SKU Description	Market Price	ACS Price
FC	1-10-FEDR1-377-01-12	FortiEDR-25 FortiEDR Discover, Protect	\$2,550.00	\$2,167.50



## V. Waterfall Pricing

Managed FortiEDR Pricing		
Devices	Subsequent Pricing	Initial Pricing
0-1000	\$53.11	\$56.99
1001-2000	\$49.23	\$53.11
2001-3000	\$45.35	\$49.23
3001-5000	\$42.48	\$45.35
5001+	\$41.49	\$42.48

Additional products or services offered to state agencies at a minimum of a 3% discount.

## Vii. Value-Added Services

### Managed Detection and Response (INCLUDED IN PRICING)

We made the decision to offer our low price while including the U.S. based Security Operations Center (SOC) team to manage the solution. While individual customers will have full administrative access to the solution, our U.S. team is there to respond and answer any questions 24/7/365. Our already low pricing already **includes** all the MDR features listed above that were “optional” at no additional cost!

- **Enhanced Threat Detection:** A Fully Managed FortiEDR solution with EDR (Endpoint Detection and Response) capabilities offers advanced threat detection mechanisms. It continuously monitors endpoints for any suspicious activity, detecting potential threats and indicators of compromise in real-time.
- **Rapid Incident Response:** With EDR response capabilities, the FortiEDR solution enables swift incident response. It provides your administrators and our 27/7 US SOC (Security Operations Center) with actionable insights and automated response options, allowing them to quickly contain and remediate security incidents, minimizing or even eliminating the potential impact of a breach.
- **Proactive Threat Hunting:** FortiEDR's EDR response empowers administrators and our 24/7 SOC to conduct proactive threat hunting. It allows for in-depth analysis of endpoint activities, searching for hidden threats or signs of advanced persistent threats (APTs) that may have evaded traditional security measures. This proactive approach helps identify and eliminate threats before they can cause significant damage.
- **Forensic Investigation:** The EDR response functionality within FortiEDR enables detailed forensic investigation. It provides comprehensive visibility into endpoint activities, including the ability to



track and analyze the entire attack chain. This capability is invaluable for incident investigation, root cause analysis, and gathering evidence for legal or compliance purposes.

- **Endpoint Remediation:** FortiEDR's EDR response facilitates endpoint remediation by automating the process of removing malicious artifacts and restoring compromised systems to a secure state. It streamlines the remediation workflow, saving time and effort for security teams while ensuring a thorough and consistent approach.
- **Threat Intelligence Integration:** A Fully Managed FortiEDR solution with EDR response leverages threat intelligence feeds to enhance its detection capabilities. By integrating with threat intelligence platforms and leveraging up-to-date threat intelligence, we can identify and respond to emerging threats faster, ensuring proactive protection against the latest attack techniques.
- **Centralized Management and Reporting:** With a Fully Managed FortiEDR solution, EDR response operations can be centrally managed. Administrators and our SOC team can oversee and control endpoint security measures from a unified dashboard, allowing for streamlined management and reporting across the state. This centralized approach simplifies administration, monitoring, and compliance reporting.
- **Continuous Monitoring and Protection:** FortiEDR's EDR response capabilities provide continuous monitoring and protection for endpoints. It monitors endpoint activities in real-time, detecting threats and suspicious behaviors promptly. This proactive monitoring ensures a high level of security against evolving threats, minimizing the risk of successful attacks.
- **Compliance and Audit Readiness:** A Fully Managed FortiEDR solution with EDR response helps organizations meet compliance requirements and maintain audit readiness. It offers robust endpoint security measures, comprehensive incident response capabilities, and reporting, enabling organizations to demonstrate their adherence to regulations and security best practices.

## Achieving the 99.999% Uptime

FortiEDR maintained an uptime of 99.999% in 2020-2021. While in 2022, the uptime dipped slightly to 99.99% but still maintains an impressive track record! In order to achieve 99.999% we have datacenters in multiple, geographically dispersed U.S. locations hosting multiple redundant and load balanced copies of FortiEDR. Monitored by our U.S. based SOC (Security Operations Center).

FortiEDR uses a variety of techniques to maintain its high uptime, including:

- **Redundancy:** FortiEDR is deployed in a redundant configuration, with multiple appliances providing coverage for each endpoint in multiple datacenters. This helps to ensure that there is always an appliance available to protect endpoints, even if one appliance fails.
- **Load balancing:** FortiEDR is deployed in a load-balanced configuration, with multiple appliances sharing the workload of protecting endpoints. This helps to improve performance and can also help to prevent outages if one appliance fails.

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution





- Failover: FortiEDR is configured to automatically fail over to a backup appliance or datacenter if the primary appliance or datacenter becomes unavailable. This helps to ensure that endpoint protection is always available, even if there is an outage.

## Optional Added Services

### On-Site Training

On-site Training priced at a one-time \$6,000 1-day session.

- Details
  - Tailored Training Experience: On-site training allows organizations to customize the training program to meet their specific needs. Training providers can work closely with the organization to understand their goals, challenges, and desired outcomes, and design a curriculum accordingly.
  - In-person Interaction: With on-site training, participants have direct access to instructors who can provide real-time guidance, answer questions, and facilitate discussions. This interactive environment promotes engagement and fosters a deeper understanding of the subject matter.
  - Practical Application: On-site training incorporates practical exercises and simulations that allow participants to apply their knowledge in real-world scenarios. This hands-on approach enhances the learning experience and helps participants gain practical skills that can be immediately implemented in their work environment.
  - Team Building and Collaboration: On-site training brings employees together in a shared learning environment. It encourages collaboration, teamwork, and the exchange of ideas and experiences among participants. This can foster a sense of camaraderie and strengthen working relationships within the organization.
  - Focus and Concentration: On-site training provides a dedicated learning environment, free from distractions commonly found in the workplace. Participants can fully immerse themselves in the training material, ensuring maximum focus and concentration.
  - Contextualized Examples: On-site training can be customized to include examples relevant to the organization's industry, challenges, and specific use cases. This helps participants relate the training material to their own work environment and enhances the applicability of the knowledge gained.
  - Flexibility and Adaptability: On-site training can be scheduled at a time that is convenient for the organization, taking into account operational requirements and employee



availability. The training provider can adapt the program based on the participants' skill levels and adjust the pace to ensure effective learning.

- Personalized Support: On-site training offers the opportunity for personalized support and one-on-one interactions with instructors. Participants can receive individualized guidance, address specific questions or concerns, and receive immediate feedback, enhancing their learning experience.
- Cost-Effective for Larger Groups: On-site training can be cost-effective for organizations with a larger number of participants. Instead of sending employees to external training programs individually, the organization can leverage economies of scale by hosting the training on-site for a larger group.

## Managed & Monitored FortiSIEM

Pricing \$444.36/Device/Year

- Details

- Cloud-Based FortiSIEM Deployment: PCS sets up and manages the cloud infrastructure hosting FortiSIEM, relieving clients of the burden of infrastructure maintenance and management.
- Security Event Monitoring: PCS conducts continuous monitoring of clients' network, systems, and applications using FortiSIEM. They analyze security events, logs, and network flows to detect potential threats and anomalies.
- Incident Detection and Response: PCS leverages FortiSIEM to detect and respond to security incidents promptly. Their security analysts analyze events, investigate alerts, and initiate appropriate response alerts to help minimize the impact of security breaches.
- Threat Intelligence Integration: PCS integrates external threat intelligence feeds with FortiSIEM, enabling clients to benefit from up-to-date information on emerging threats, known attack vectors, and malicious actors. This integration enhances threat detection capabilities.
- Incident Detection and Alerting: PCS identifies security incidents from detection to alerting. They follow predefined alert response processes, provide emergency alerting, and escalate critical alerts to appropriate teams or individuals within the client organization.
- Compliance Monitoring and Reporting: PCS helps clients monitor compliance with industry regulations and standards. They can help configure FortiSIEM to generate compliance reports, track adherence to security policies, and support regulatory audits.

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



- Customizable Dashboards and Reporting: PCS creates customized dashboards and reports within FortiSIEM to provide clients with real-time visibility into their security posture. These dashboards and reports can be tailored to meet clients' specific requirements and provide meaningful insights.
- Log Management and Analysis: PCS manages log data collection, normalization, and analysis using FortiSIEM. They monitor logs from various sources, troubleshoot logging issues, and identify security incidents, all while ensuring efficient log management.
- Vulnerability Notifications: Using FortiSIEM, PCS notifies clients about vulnerabilities seen within their organization.
- Integration with Security Tools: PCS integrates FortiSIEM with clients' existing security tools, such as firewalls, antivirus solutions, and intrusion detection systems. This integration centralizes security information, streamlines workflows, and enhances overall security operations.
- Managed SIEM Service: PCS offers managed SIEM services, utilizing FortiSIEM as the core platform. They oversee the day-to-day operation of FortiSIEM, ensuring its performance, availability, and effectiveness in meeting clients' security monitoring needs.
- Security Consultation and Advisory Services: PCS provides security consultation and advisory services to clients, leveraging their expertise in FortiSIEM and broader security practices. They offer quarterly meetings to suggest recommendations, best practices, and guidance to enhance clients' security posture.

## Forensics and Remediation Services

Pricing \$210/hour

PCS offers a Cyber Forensics and Remediation Service that can help organizations to investigate and respond to cyber incidents. The service includes the following:

- Incident response: PCS will work with the organization to assess the incident and develop a response plan. This may include steps such as containment, eradication, and recovery.
- Forensic analysis: PCS will conduct a forensic analysis of the affected systems to gather evidence of the incident. This evidence can be used to identify the attacker, understand the attack vector, and prevent future attacks.
- Remediation: PCS will work with the organization to implement security controls to prevent future attacks. This may include steps such as patching vulnerabilities, implementing security policies, and training employees on security best practices.

PCS' Cyber Forensics and Remediation Service can help organizations to:

RFQ #: DMS-22/23-155

Endpoint Detection and Response Solution



- Minimize the impact of a cyber incident: PCS can help organizations to contain and eradicate the attack, and to recover from the incident as quickly as possible.
- Gather evidence: PCS can gather evidence of the attack, which can be used to identify the attacker and prevent future attacks.
- Implement security controls: PCS can help organizations to implement security controls to prevent future attacks.

Additional products or services offered to state agencies at a minimum of a 3% discount.

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.

PC Solutions & Integration, Inc.

Vendor Name

65-0798706

FEIN

5.16.23

Date

*Robert S. Boush*

Signature

Robert Boush

Signatory Printed Name

**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**



# Non-Disclosure Agreement

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

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

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

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

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

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

### 1. Definitions.

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



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

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

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



- (e) Storing and safeguarding the Confidential Information in a physically and electronically secure location where Access is limited to authorized persons;
  - (f) Maintaining an up-to-date list of individuals who are authorized to Access the Confidential Information;
  - (g) Instructing and requiring all individuals authorized to Access the Confidential Information to adhere to the confidentiality requirements set forth in this Agreement prior to being granted Access to the Confidential Information;
  - (h) Not allowing, through action or inaction, any Confidential Information to be sent by any medium, transmitted, or to be Accessed outside of the United States. For the purposes of this restriction, "Access" does not include remote support sessions for devices that might contain the Confidential Information; however, during the remote support session the Department requires Recipient to escort the remote support access and maintain visibility of the actions taken during the remote support access. Requests for remote access will be submitted to the Department's Contract Manager. With approval, third parties may be granted time-limited terminal service access to information technology resources as necessary for fulfillment of related responsibilities. Remote connections are subject to detailed monitoring via two-way log reviews and the use of other tools; and
  - (i) Performing all actions necessary to assist with all tasks in furtherance of the Department's efforts to comply with the obligations under Chapters 60FF and 60GG, Florida Administrative Code, as applicable.
- 6. Liability.** By signing this Agreement, Recipient acknowledges Recipient shall be responsible and liable for the acts and omissions of any of Recipient's employees and/or the Affiliate(s) that result in a violation of this Agreement as if such acts or omissions were Recipient's acts or omissions. Recipient represents that it will enter into a written agreement with an Affiliate with Access to Confidential Information wherein it shall require the Affiliate agree to be bound by and adhere to the terms of this Agreement.
- 7. Notice of Breach.** Recipient must notify the Department as expeditiously as practicable, but in all instances no later than within one (1) business day, in the event Recipient discovers any incident that involves, or which Recipient reasonably believes may involve, a breach of the Confidential Information which includes any unauthorized Access to or disclosure of the Confidential Information and/or which compromises the security, integrity, or confidentiality of the Confidential Information. Additionally, if the Department or Customer shares with Recipient information that is covered by section 501.171, F.S., Recipient is responsible for fulfilling all applicable requirements of section 501.171, F.S., including those that would otherwise be the responsibility of the Department or Customer. Recipient agrees to provide the Department and applicable Customers with all details associated with all breaches or suspected breaches and to work with the Department or the applicable Customer to investigate and resolve any breach, implement any necessary remedial measures, and perform all tasks to ensure full compliance with section 501.171, F.S., including, where applicable, providing any breach notifications to comply with this statutory requirement.
- 8. Indemnification.** Recipient shall defend, indemnify, and hold harmless the Department, the Customer, and the State against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, in connection with any third-party claim, suit, action, or proceeding arising out of or resulting from a violation of any obligation set forth in this Agreement by Recipient (including its employees) or its Affiliates. The Agreement does not constitute a waiver of sovereign immunity or consent by the Department, Customers, or the State or its subdivisions to suit by third parties. The obligations of this paragraph shall survive the Agreement.



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

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

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

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

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





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

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

**FLORIDA DEPARTMENT OF MANAGEMENT SERVICES**

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

By: David H. Rudnick  
Name: David Rudnick  
Title: Vice President  
Date: 5.16.23

## Partnerships (Subcontractors)

The below will identify all subcontractors the vendors will utilize to provide the services required by this RFQ and what services each subcontractor will provide.

### PCS and SkyHelm Partnership

Skyhelm is one of PCS’ strategic partners. This partnership between PCS and SkyHelm was formed to deliver specialized security services to bring the strengths of the two companies together and be able to service our clients better. SkyHelm’s mission is to protect America’s critical infrastructure technology. Our combined teams are passionate about solving complex technology challenges by focusing on the outcomes our customers care about and by applying our extensive industry-specific experience. Together with your team, we design, implement, and manage complete cybersecurity and infrastructure technology solutions for organizations like municipalities, public safety, utilities, and more.