

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

**AGENCY TERM CONTRACT
FOR
NETWORK-BASED ASSET DISCOVERY (AGENTLESS)
DMS-22/23-154C
BETWEEN
STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES
AND
ST. LOUIS BASED WORLD WIDE TECHNOLOGY, INC.**

AGENCY TERM CONTRACT

This Contract is between the STATE OF FLORIDA, DEPARTMENT OF MANAGEMENT SERVICES ON BEHALF OF FLORIDA DIGITAL SERVICE (Department), with offices at 4050 Esplanade Way, Tallahassee, Florida 32399-0950, and ST. LOUIS BASED WORLD WIDE TECHNOLOGY, INC. (Contractor), with offices at 1 World Wide Way, St. Louis, MO 63146, 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-22/23-154, Network-Based Asset Discovery (Agentless) Solution; and

WHEREAS, the Department has accepted the Contractor's Quote and enters into this Contract in accordance with the terms and conditions of RFQ No. DMS-22/23-154.

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-22/23-154;
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-22/23-154 shall control.

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

6.0 Amendments

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

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

7.0 Contract Notices

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

8.0 Contract Contacts

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

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

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

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

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

8.2 The Department's Contract Manager is:

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

The Contract Manager will perform the following functions:

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

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

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

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

Carol Harting
Business Development Manager
1 World Wide Way
St. Louis, MO 63146
Telephone: (314) 995-6103
Email: carol.harting@wwt.com

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

9.0 Assignment

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

10.0 Price Decreases

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

11.0 Additions/Deletions

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

12.0 Cooperative Purchasing

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

13.0 Other Conditions

13.1 Independent Contractor Status

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

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

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

13.2 Force Majeure

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

13.3 Cooperation with the Florida Senate and Florida House of Representatives

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

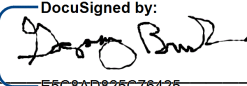
13.4 Employment of State Workers

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

SIGNATURE PAGE IMMEDIATELY FOLLOWS

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

ST. LOUIS BASED WORLD WIDE
TECHNOLOGY, INC.:

DocuSigned by:

E5C8AD825C78425...
Authorized Signature

Greg Brush

Print Name

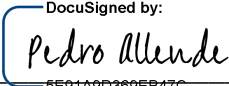
AVP Public Sector

Title

6/29/2023 | 9:44 PM CDT

Date

STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES:

DocuSigned by:

5E91A9D389EB47C...
Pedro Allende, Secretary

6/30/2023 | 7:40 AM EDT

Date

Exhibit A
Request for Quotes (RFQ)
DMS-22/23-154
Network-Based Asset Discovery (Agentless)
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 (PO): 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: The network-based asset discovery (agentless) solution that aggregates and analyzes data to provide a holistic view of an organization's assets. The Solution shall

catalogue each device on a network without the use or installation of an agent or software onto each individual device.

2.0 OBJECTIVE

Pursuant to section 287.056(2), F.S., the Department intends to purchase a network-based asset discovery (agentless) Solution for use by the Department and Customers to identify and manage each device on a network without the use or installation of an agent or software onto each individual device as specified in this RFQ.

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

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

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

3.0 DESCRIPTION OF PURCHASE

The Department is seeking a Contractor(s) to provide a network-based asset discovery (agentless) 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

Any POs issued pursuant to the RFQ will have the term identified in the PO. 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.

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 enable the process of cataloguing each device on a network, without the use or installation of an agent or software onto each individual device. The Solution shall provide for agentless asset identification whereby the packet and communications of a device is analyzed. The Solution shall inspect communication flows, and the application packets themselves to determine make, model, software load, and even serial numbers, all without installation of an agent. The Solution shall provide for additional enrichment of this data, and further classification by machine learning and compared to a catalog of millions of devices allows for accurate device identification and classification.

6.1.1. Multi-Tenancy Support

The Solution shall be designed to support multiple tenants, allowing the end user to manage devices and policies across different organizations or customer groups. This should include role-based access control to ensure that each tenant can only view and manage their own devices.

6.1.2. Agentless Approach

The Solution shall provide the ability to discover and query endpoints without requiring the installation of agents on each device. This can simplify deployment and reduce the impact on device performance and security. This also allows for discovery of a broad range of assets and vulnerabilities.

6.1.3. Discovery for Multiple Endpoint Types

The Solution shall discover a wide range of endpoints, including desktops, laptops, servers, mobile devices, and IoT devices.

6.1.4. 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. This allows capacity extensibility in the cloud with minimal impact on agent or management infrastructure.

6.1.5. Remote Management

The Solution shall provide the ability to identify all networked devices and enforce policies remotely, without the need for direct physical access. This may include tasks such as software installation, patching, and configuration management.

6.1.6. Data Security

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

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

6.1.7. Compliance and Third-Party Certification

The Solution shall comply with relevant state and federal laws and standards such as the Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, Driver Privacy Protection Act, General Data Protection Regulation, and third-party certifications such as SOC 2 and ISO 27001. The Department, Purchaser, or Customer may require awarded Vendors(s) to execute security agreements, including but not limited to, Criminal Justice Information System (CJIS) riders or Business Associate Agreements as a condition of performance or purchase order issuance.

6.1.8. Security Features

The Solution shall provide the ability to work in conjunction with robust security features to protect against threats like malware, data breaches, and unauthorized access. This shall include, but not be limited to, endpoint protection, firewalls, and encryption.

6.1.9. Reporting and Analytics

The Solution shall provide detailed reporting and analytics to help monitor device health, track compliance with policies, and identify potential issues or risks. The selected Solution shall have the capacity to provide ad-hoc reports to Purchasers and Customers.

6.1.10. Integration with Other Tools

The Solution shall support dynamic policy and contextual access and other novel authentication methods.

6.1.11. Scalability

The Solution shall provide the ability to scale to meet the needs of the organization as it grows, without diminishing the ability to adequately manage growing numbers of endpoints.

6.1.12. 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.

6.1.13. Ease of Use

The Solution shall be easy to use and configure, with an intuitive graphical user interface and clear documentation and support resources which instruct on use of the Solution.

6.1.14. Configuration Tools and Customization

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

6.1.15. Data Migration Services

The Solution shall provide data migration services to ensure a smooth transition of data from a Customer or Purchaser's current system to the Contractor's Solution.

6.1.16. Disaster Recovery Services

In the event of a disaster or system failure, the Solution shall provide disaster recovery services, including backup and a disaster recovery plan ensuring business continuity.

6.1.17. Role-Based Access

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

6.1.18. 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.

6.1.19. Integration

- 6.1.19.1.** The Solution shall integrate with the Department's existing security tools such as firewalls, endpoint management solutions, and security information and event management (SIEM) systems. Each Customer shall determine if the Solution is able to integrate with their security tools. The Contractor shall take any steps necessary to support Customer integration.
- 6.1.19.2.** The Solution shall be capable of data integration through common exchange techniques and frameworks such as RESTful APIs.
- 6.1.19.3.** The Solution shall be capable of integrating with a variety of identity and access management (IAM) systems to meet Customer current and future needs.
- 6.1.19.4.** Initial integration shall include connecting a Customer, upon request, to the State Cybersecurity Operations Center (CSOC) and validating with FL[DS] that all Solution data is properly integrated.
- 6.1.19.5.** Integration maintenance may be required after initial integration to ensure that the Solution properly exchanges data between a Customer and the CSOC. The Contractor shall address any concerns that FL[DS] has regarding integration issues.

6.1.20. Performance and Availability

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

- 6.1.20.1.** The performance and availability SLA shall provide information on performance and availability objectives for the Solution to perform successfully and be available 99.999% of the time per month.
- 6.1.20.2.** The Contractor 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 the Department, Purchaser, and Customer to ensure all Parties have all 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 (e.g., in-person, live webinar, online course), specific training suggested for each user roles.
 - 6.2.2.1. The training SLA must specify what is included within the Initial Training (included in Item No. 1 on Attachment A, Price Sheet) provided and Ongoing Training (including scope and frequency) 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 performance 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. The kickoff meeting shall be held in accordance with the deliverables herein.
- 6.3.3. The kickoff meeting for the Customer(s) should include a demonstration of the Solution, or prior to the kickoff meeting, a link may be provided to the Customer(s) to demonstrate the Solution.

6.4. **Implementation**

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

The Implementation Plan must include the following at a minimum:

- 6.4.1. All tasks required to fully implement and complete initial integration of the Solution.
- 6.4.2. Identify the entity responsible for each task (e.g., Contractor, Purchaser, FL[DS] (if applicable), or other Customer).
- 6.4.3. Date 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. The vendor shall 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.

**TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES**

No.	Deliverable	Time Frame	Financial Consequences
2	The Contractor shall submit the Implementation Plan timely and in accordance with the PO and any applicable ATC.	The Contractor shall collaborate with the Customer and submit each Customer's Implementation Plan to the Purchaser and each additional Customer within 10 calendar days of PO issuance.	<p>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.</p> <p>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.</p>
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.	<p>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.</p> <p>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.</p>

**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.

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 network-based asset discovery (agentless) 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 30.5.
- 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) Document any substantial deviations within Vendor’s Solution from the Scope of Work.
 - 5) Detail regarding any value-added services.
 - 6) **Attachment A**, Price Sheet, containing pricing for all items and completed in accordance with the instructions provided in this RFQ.
 - 7) **Attachment B**, Contact Information Sheet, containing the contacts for the Quote and the resulting ATC(s) and PO(s).
 - 8) **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 8, 2023
Pre-Quote Conference Link: https://us02web.zoom.us/meeting/register/tZ0ufu2gqzlpGdQ3U_xdCXnrvtRQ2XSXqu_	May 11, 2023, at 9:00 a.m., Eastern Time
Responses Due to the Procurement Officer, via email	May 17, 2023, by 5:00 p.m., Eastern Time

EVENT	DATE
Solution Demonstrations and Quote Negotiations	May 18-22, 2023
Anticipated Award, via email	May 22, 2023

12.0 PROCUREMENT OFFICER

The Procurement Officer for this RFQ is:

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

13.0 PRE-QUOTE CONFERENCE

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

14.0 SOLUTION DEMONSTRATIONS

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

15.0 QUOTE NEGOTIATIONS

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

16.0 SELECTION OF AWARD

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

17.0 RFQ HIERARCHY

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

- 1) The PO(s);
- 2) The ATC(s);
- 3) The Department's Non-Disclosure Agreement (NDA) or other Purchaser's NDA;
- 4) This RFQ;
- 5) Department's Purchase Order Terms and Conditions;

- 6) The ACS contract the vendor submitted their Quote in accordance with [ACS: Cloud Solutions (43230000-NASPO-16-ACS), Software Value Added Reseller (SVAR) (43230000-23-NASPO-ACS), or Technology Products, Services, Solutions, and Related Products and Services (43210000-US-16-ACS)]; and
- 7) The vendor's Quote.

18.0 DEPARTMENT'S CONTRACT MANAGER

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

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

19.0 PAYMENT

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

20.0 PUBLIC RECORDS AND DOCUMENT MANAGEMENT

20.1 Access to Public Records

The Department may unilaterally cancel any applicable ATC or PO for failure by the Contractor to comply with this section by not allowing access to all public records, as

defined in Chapter 119, F.S., made or received by the Contractor in conjunction with any applicable ATC or PO.

20.2 Contractor as Agent

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

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

DEPARTMENT:

CUSTODIAN OF PUBLIC RECORDS

PHONE NUMBER: 850-487-1082

EMAIL: PublicRecords@dms.fl.gov

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

OTHER PURCHASER:

CONTRACT MANAGER SPECIFIED ON THE PO

20.3 Public Records Exemption

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

20.4 Document Management

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

21.0 IDENTIFICATION AND PROTECTION OF CONFIDENTIAL INFORMATION

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

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

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

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

22.0 USE OF SUBCONTRACTORS

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

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

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

23.0 LEGISLATIVE APPROPRIATION

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

24.0 MODIFICATIONS

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

25.0 CONFLICT OF INTEREST

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

26.0 DISCRIMINATORY, CONVICTED AND ANTITRUST VENDORS LISTS

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

27.0 E-VERIFY

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

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

28.0 COOPERATION WITH INSPECTOR GENERAL

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

29.0 ACCESSIBILITY

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

30.0 PRODUCTION AND INSPECTION

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

31.0 SCRUTINIZED COMPANIES

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

Companies that Boycott Israel List”) or becomes engaged in a boycott of Israel. The State Board of Administration maintains the “Quarterly List of Scrutinized Companies that Boycott Israel” at the following link:

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

32.0 BACKGROUND SCREENING

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

32.1 Background Check

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

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

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

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

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

32.2 Disqualifying Offenses

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

Contractor is required to immediately remove that Person from any position with access to State of Florida Data or directly performing services under the Contract. The disqualifying offenses are:

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

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

32.3 Refresh Screening

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

32.4 Self-Disclosure

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

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

32.5 Duty to Provide Security Data

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

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

32.6 Screening Compliance Audits and Security Inspections

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

32.7 Record Retention

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

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

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

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

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

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

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

32.8 Indemnification

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

33.0 LOCATION OF DATA

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

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

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

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

34.0 DATA TRANSMISSION

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

35.0 TERMS AND CONDITIONS

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

36.0 COOPERATIVE PURCHASING

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

37.0 PRICE ADJUSTMENTS

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

38.0 FINANCIAL STABILITY

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

39.0 RFQ ATTACHMENTS

Attachment A, Price Sheet

Attachment B, Contact Information Sheet

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

Department's Purchase Order Terms and Conditions

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

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT A PRICE SHEET

I. Alternate Contract Source (ACS)

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

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

_____ 43230000-NASPO-16-ACS Cloud Solutions

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

II. Pricing Instructions

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

III. Pricing

Initial Term Pricing (Years 1-3)

Item No.	Description	Rate Per User (A)
1	<p><u>Initial Software Year</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include:</p> <ul style="list-style-type: none"> • Implementation • initial training • Initial Integration • integration maintenance • support services 	\$ _____
2	<p><u>Subsequent Software Year</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ _____

Optional Renewal Term Pricing (Years 4-6)

Item No.	Description	Rate Per User (A)
1	<p><u>Initial Software Year</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include:</p> <ul style="list-style-type: none"> • Implementation • initial training • Initial Integration • integration maintenance • support services 	\$ _____
2	<p><u>Subsequent Software Year</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ _____

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 network-based asset discovery (Agentless), 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 29.0**, Scrutinized Companies, a vendor submitting a Quote must certify that their company is not participating in a boycott of Israel. By signing below, the vendor so certifies. Additionally, the person submitting the quote and pricing is authorized to respond to this RFQ on the vendor’s behalf, as confirmed by the signature below.

Vendor Name

Signature

FEIN

Signatory Printed Name

Date

ATTACHMENT B CONTACT INFORMATION SHEET

I. Contact Instructions

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

II. Contact Information

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

Exhibit B
Contractor's Quote



The State of Florida

Department of Management Services

Network-Based Asset Discovery (Agentless) Solution

RFQ Number DMS-22/23-154

Cloud Solutions (43230000-NASPO-16-ACS)

May 17, 2023

Presented by
Perry Bright
Client Manager
World Wide Technology
850-803-0076
Perry.Bright@wwt.com

wwt.com

The State of Florida Department of Management Services
May 17, 2023



May 17, 2023

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

RE: WWT Response to The State of Florida Department of Management Services Request for Quote (RFQ) for Network-Based Asset Discovery (Agentless) Solution

Dear Ms. Morgan:

World Wide Technology (WWT) thanks the State of Florida, Department of Managed Services (the Department) for the invitation to present our solution that meets or exceeds the software, implementation, training, support and integration services requirements of RFQ DMS-22/23-154 and bolsters the Department's Enterprise Cybersecurity Resiliency Program as a model for the nation.

WWT's solution applies enterprise wide and adheres to multiple compliance standards

For this Network-Based Asset Discovery project, WWT provides comprehensive, centralized agentless visibility into the Department's systems to manage devices and policies across different organizations or customer groups. This solution enables monitoring, reporting and analytics, data sharing management, encryption, cloud and remote management, scalability, integration and all other requirements listed in Section 6.0 Scope of Work in a multi-tenancy infrastructure to ensure that each tenant only views and manages their own devices. Also, our proposal creates a consortium contract that provides access to waterfall pricing for city, county and state agency security needs, empowering lower revenue-generating cities and counties to affordably perform these functions and comply with state standards.

Our holistic plan mirrors the successful approach WWT currently employs for RFP DMS-21/22-240 Asset Discovery Software and Support. This includes ensuring compliance with the State and Local Government Cybersecurity Acts, General Appropriations Act, National Institute of Standards and Technology Cybersecurity Framework (NIST) standards and February 2021 Florida Cybersecurity Task Force Final Report findings while guarding against conflicts with Chapter 282 Florida Statutes, Rule Title 60GG, Florida Administrative Code (F.A.C.) and other cybersecurity best practices.

Our staff's wide-ranging experience with sensitive security projects ensures an innovative and collaborative approach to mature the Department's security architecture and capabilities

WWT is a global technology solutions provider with eleven technology and business services practices. Our security practice generates more than \$2 billion in revenue through implementing security services, advisory services, product integrations and other solutions for global customers. Our team includes more than 200 former CISOs, CIOs, security analysts, architects, engineers, application developers and industry-certified professionals from some of the most reputable security companies and most sensitive customer environments in the world. This team brings strong security knowledge, experience and program management capabilities that drive your Network-Based Asset Discovery (Agentless) timelines, manage SLAs and accelerate security and business outcomes.

A contributing factor to this success is our system integrator role in working with leading cybersecurity cloud and software companies to provide solutions. WWT has strategically chosen to partner with Foresite and Tenable for this RFQ. Our collaborative approach involves a comprehensive reach across

The State of Florida Department of Management Services
May 17, 2023



other critical technology stacks that include Cloud, AI, Digital, Application Development / Management, Networking, Storage and more to recommend solutions, integrations and automations to optimize the Department's return on investment and mature the State's security architecture.

WWT sandbox environments validate current and future use cases and security features

WWT has hundreds of Advanced Technology Center (ATC) labs that the Department and its customers can utilize to drive knowledge on specific security products, test use cases, integrate solutions together and increase adoption across the State.

We have created custom integrated labs for customers with Tenable and other security solutions to provide robust security features (e.g., endpoint protection, firewalls and encryption) that protect against threats like malware, data breaches, and unauthorized access. These labs also facilitate integration, configuration, customization, data migration, disaster recovery, role-based access and data export methodologies to drive testing and secure outcomes.

WWT's past accomplishments with security projects assure the success of DMS-22/23-154

Given that the Department plans to launch many security projects at the same time, our WWT Program Management capabilities enable us to run multiple projects simultaneously and pull in resources to scale and meet project timelines and deliver with excellence. The WWT team has many templates and documents from prior engagements around the program management and security solutions that can be leveraged and customized for the Department and customers to optimize implementation times and reduce resource requirements and meetings for the Department and its customers.

Having implemented similar strategies for other projects, the following illustrates the type of success that the Department can experience with WWT as its trusted advisor for this project:

- Scanned thousands of customer IP addresses to identify and remediate vulnerabilities
- Managing almost a million end points for a Tanium customer globally
- Implemented Tenable, Rapid7 and similar solutions for vulnerability scanning and remediation
- Developed and operationalized a rapid vulnerability remediation program to reduce risk

WWT believes in the power of uniting employees, customers, partners and communities against cyber threats. As adversaries become more cunning, skilled and innovative, WWT has deep experience in collaborating with the State of Florida, technology vendors, customers and other integrators to increase security maturity and capabilities. From Tallahassee to Key West, Florida, WWT wants to collaborate on the Network-Based Asset Discovery (Agentless) project to secure, all together across the entire state.

Please call me at 850-803-0076 to discuss any questions or comments about this proposal. Again, thank you for this opportunity.

Respectfully,

Perry Bright

Perry Bright
Client Manager
Perry.Bright@wwt.com



Table of Contents

10.0 RESPONSE CONTENT AND FORMAT.....	2
---------------------------------------	---

10.0 RESPONSE CONTENT AND FORMAT

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

1) Documentation to describe the network-based asset discovery (agentless) Solution proposed and how it meets the requirements of this RFQ to include the following at a minimum:

Tenable Vulnerability Management (Tenable.io), gives you a risk-based view of your entire attack surface- from IT to cloud to OT and containers- so you can quickly identify, investigate and prioritize vulnerabilities. You get immediate visibility so you can understand your risk and know which vulnerabilities to fix first.

Powered by Nessus technology and managed in the cloud, Tenable.io provides the industry's most comprehensive vulnerability coverage with the ability to predict which security issues to remediate first. Using an advanced asset identification algorithm, Tenable.io provides the most accurate information about dynamic assets and vulnerabilities in ever-changing environments. As a cloud-delivered solution, its intuitive dashboard visualizations, comprehensive risk-based prioritization, and seamless integration with third-party solutions help security teams maximize efficiency and scale for greater productivity. Tenable.io™ brings an effective approach to solve today's toughest vulnerability management challenges. Using an advanced asset identification algorithm, Tenable.io provides the most accurate information about dynamic assets and vulnerabilities in ever-changing environments.

Key benefits include:

- **Continuous Vulnerability:** Eliminate blind spots by continuously track known and unknown assets and their vulnerabilities. Identify threats and unexpected network changes before they turn into breaches.
- **Boost Productivity:** Take advantage of the SaaS-based solution to run your initial assessments in less than 5 minutes without the IT hardware or maintenance burden.
- **Prioritize Risks:** Combine vulnerability data, threat intelligence and data science for easy-to-understand risk scores to quickly identify the highest business risk.
- **Automate Processes:** Leverage a fully documented API and pre-built integrations to import third-party data, automate scans, and share data with your IT systems.
- **Maximize ROI:** Eliminate double- or triple-counting of assets that have multiple IP addresses with the industry's first asset-based licensing model.

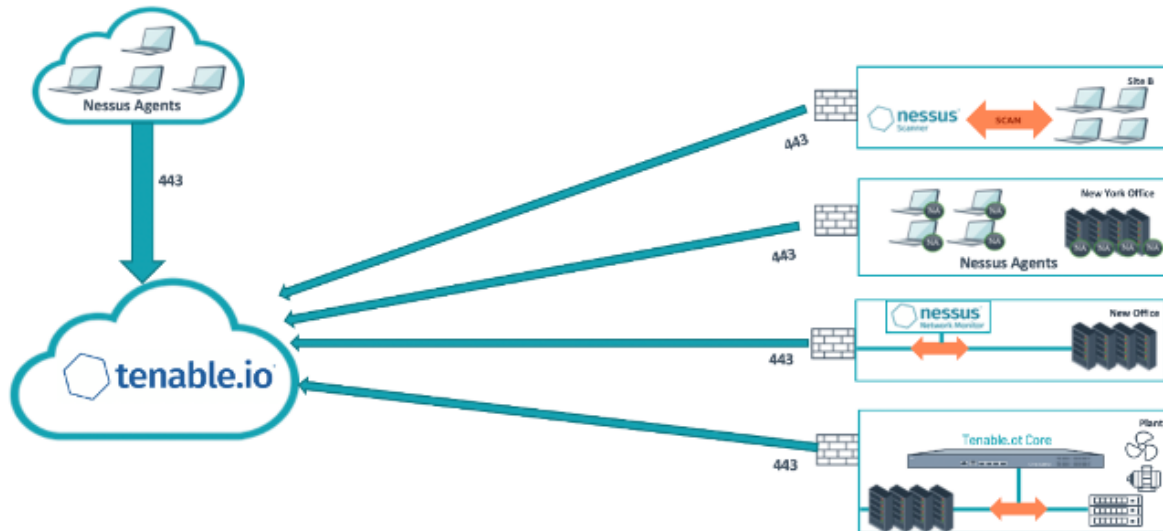
As a cloud-delivered solution, its simple, "data-comes-to-you" interface, intuitive templates and guidance, and seamless integration with third-party solutions help security teams maximize efficiency and scale for greater productivity. When visibility and insight matter most, Tenable.io helps you focus on the right action every time.

Deployment Architecture

Tenable.io is a cloud-based platform that serves as a centralized management console for associated modules. Tenable.io modular applications address specific security needs, including Tenable.io Vulnerability Management, Tenable.io Web Application Scanning and Tenable.cs. Tenable.io applications can be licensed individually; there are no prerequisites or co-purchase requirements (except for PCI ASV add-on module).

The scanners that accompany Tenable.io include Nessus Scanners, Nessus Agents, and Nessus Network Monitor, which are installed on premise, within your infrastructure. All traffic is outbound only and the scanners report their findings to the Tenable.io management console.

Tenable.io: Converged Deployment



The sensors that connect to the platform play a major role in a customer's security, collecting vulnerability and asset information. Protecting this data and ensuring the communication paths are secure is a core function of the Tenable.io. Tenable.io supports several sensors today: Nessus vulnerability scanners, Passive scanners and Nessus Agents.

These sensors connect to the Tenable.io platform after cryptographically authenticating and linking to Tenable.io. Once linked, Tenable.io manages all updates (plugins, code, etc.) to ensure the sensors are always up to date.

Traffic from the sensors to the platform is always initiated by the sensor and is outbound-only over port 443. Traffic is encrypted via SSL communication using TLS 1.2 with a 4096-bit key. This removes the need for firewall changes and allows the customer to control the connections via firewall rules.

- Scanner-to-platform authentication
 - The platform generates a random key of 256 bit length for each scanner connected to the container and passes that key to scanner during the linking process
 - Scanners uses this key to authenticate back to the controller when requesting jobs, plugin updates and updates to the scanner binary
- Scanner-to-platform job communication
 - Scanners contact the platform every 30 seconds
 - If there is a job, the platform generates a random key of 128-bits
 - The scanner requests the policy from the platform
 - The controller uses the key to encrypt the policy, which includes the credentials to be used during the scan

6.1.1. Multi-Tenancy Support

The Solution shall be designed to support multiple tenants, allowing the end user to manage devices and policies across different organizations or customer groups. This should include role-based access control to ensure that each tenant can only view and manage their own devices.

Tenable IO is a multi-tenant SaaS solution that secures tenant isolation at the Container Layer. Each customer's data is marked with a "container ID," which corresponds to a specific customer subscription. This container ID assures that access to a customer's data is limited to only that customer.

6.1.2. Agentless Approach

The Solution shall provide the ability to discover and query endpoints without requiring the installation of agents on each device. This can simplify deployment and reduce the impact on device performance and security. This also allows for discovery of a broad range of assets and vulnerabilities.

Tenable IO has the ability to leverage network-based scanners to assess (discover and query) endpoints without requiring the installation of agents on the devices. The scanners and other sensors Tenable.io uses are capable of assessing many types of assets, including PCs, Network infrastructure equipment and more

6.1.3. Discovery for Multiple Endpoint Types

The Solution shall discover a wide range of endpoints, including desktops, laptops, servers, mobile devices, and IoT devices.

Tenable IO can detect most types of endpoints, including desktops, laptops, servers, mobile devices, IoT, network infrastructure and the like.

6.1.4. 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. This allows capacity extensibility in the cloud with minimal impact on agent or management infrastructure.

Tenable.io is a cloud-based Software as a Service (SaaS) offering, and updates and new releases are managed by Tenable. Local sensors attached to Tenable.io can be managed automatically by the cloud infrastructure.

6.1.5. Remote Management

The Solution shall provide the ability to identify all networked devices and enforce policies remotely, without the need for direct physical access. This may include tasks such as software installation, patching, and configuration management.

Tenable.io can detect networked devices without direct physical access, using access over the customer network. Tenable.io is used for detection of vulnerabilities and compliance issues, and does not have software installation, patching or configuration capabilities. It does integrate with a number of vendors that provide these services.

6.1.6. Data Security

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

All data is encrypted in storage and in transit: At rest, all customer data collected are encrypted using AES-256 encryption. Data in transit is encrypted using TLS v1.2 with a 4096-bit key. This includes browser, API and intra-application communication.

Multiple keys are used to encrypt data, and they are unique to the database, site, or storage location and layer. All sensitive data must be encrypted by policy, and key management processes for storage, rotation, and access are in place. Tenable uses AWS Key Management Service and keys are stored in Amazon Web Services (AWS).

- Keys are rotated annually or when there is a requirement to do so.
- Backups are encrypted when stored on AWS S3 (Simple Storage Service). AWS S3 is encrypted using SSE (Server Side Encryption) with 256-bit Advanced Encryption Standard. Reference: <http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

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

Tenable IO can do this.

6.1.7. Compliance and Third-Party Certification

The Solution shall comply with relevant state and federal laws and standards such as the Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, Driver Privacy Protection Act, General Data Protection Regulation, and third-party certifications such as SOC 2 and ISO 27001. The Department, Purchaser, or Customer may require awarded Vendors(s) to execute security agreements, including but not limited to, Criminal Justice Information System (CJIS) riders or Business Associate Agreements as a condition of performance or purchase order issuance.

Tenable's solutions comply with corporate and regulatory policies such as PCI, HIPAA, NERC and FISMA, among others. A summary of our compliance can be viewed at: <https://www.tenable.com/trust-and-assurance>

Tenable is ISO 27001 certified. See details here; <https://www.schellman.com/certificate-directory>

Tenable.io does not store or process HIPAA data; Tenable is not a "Business Associate" under the terms of HIPAA. However, the data hosting provider, AWS, is: <https://aws.amazon.com/compliance/hipaa-compliance/>

6.1.8. Security Features

The Solution shall provide the ability to work in conjunction with robust security features to protect against threats like malware, data breaches, and unauthorized access. This shall include, but not be limited to, endpoint protection, firewalls, and encryption.

6.1.9. Reporting and Analytics

The Solution shall provide detailed reporting and analytics to help monitor device health, track compliance with policies, and identify potential issues or risks. The selected Solution shall have the capacity to provide ad- hoc reports to Purchasers and Customers.

Tenable.io has a flexible report generation build process, we can also save custom reports, assisting with repetitive tasks.

Tenable.io uses a static Severity (CVSS) and a dynamic Vulnerability Priority Rating (VPR) to quantify how urgently you should remediate a vulnerability. The VPR score is the output of Tenable's industry-leading Predictive Prioritization functionality, which boils down 150 data points from various threat intelligence feeds to inform you of what is most likely to be exploited and have the greatest impact in the next 28 days.

Static: Tenable assigns all vulnerabilities a static severity based on the vulnerability's CVSS score. CVSS severity is selectable and allows either CVSSv2 or CVSSv3 to be shown as the default severity.

VPR: The VPR is a dynamic companion to the static data provided by the vulnerability's CVSSv2 score and severity, since Tenable updates the VPR to reflect the current threat landscape. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit.

For each vulnerability found, we provide detail description of the issue, a solution for how to remediate, output from the host as validation of the issue, plugin information, CVSS detail with score and indices and reference material to better understand the vulnerability. Tenable.io provides a method for filtering down upon various vulnerability/asset attributes which are best tailored around the customer's specific environment and needs. Tenable also provides report templates for exporting vulnerabilities for specific assets or all asset to the asset owners for remediation.

6.1.10. Integration with Other Tools

The Solution shall support dynamic policy and contextual access and other novel authentication methods.

Tenable.io ticket notifications can be generated from an external ticket management system after integration with the Tenable.io API. Tenable has done integrations for customers using ServiceNow, Remedy, JIRA, and other ticket systems can be done.

Tenable.io integrates with excellent solutions like ServiceNow and Jira, providing a more effective approach for end-to-end vulnerability remediation. We focus on providing the most valuable VM and Cyber Exposure solutions, and integrating with the technologies customer are already using. Tenable is committed to helping you get maximum value from your existing technology solutions, including ticketing/workflow solutions from ServiceNow, Jira (Atlassian), and BMC.

Tenable is a Silver level Technology Partner of ServiceNow – the only security partner at that level. Tenable is one of 3 Technology Partners with whom ServiceNow actively goes to market, including significant investment across product, marketing, and sales organizations. We have invested significant resources in deep and comprehensive integrations between our solutions and ServiceNow. Our integrations provide a consistent feature set and experience across Tenable integrations for ServiceNow Security Operations Vulnerability Response, ITSM, and CMDB. The integration apps install quickly out-of-the box and customers can be up and running within hours. Our solutions also offer the flexibility to customize field mapping and workflows, and these customizations remain intact after upgrades.

Tenable also integrates with Atlassian's Jira On Prem, Jira Cloud, Jira Core, Jira Software and Jira Service Desk to automatically open tickets for vulnerabilities that Tenable identifies and close them once they have been resolved, providing a cohesive and trackable remediation process.

While Tenable provides direct out-of-the-box integrations with multiple solutions, Tenable.io also has an open API which allows for custom integrations, scripts and workflows to be developed. Tenable Professional Services can also provide custom integration services if there aren't sufficient internal resources to develop the custom scripts.

6.1.11. Scalability

The Solution shall provide the ability to scale to meet the needs of the organization as it grows, without diminishing the ability to adequately manage growing numbers of endpoints.

Tenable.io is architected from the ground up as a true cloud platform. The platform is hosted by AWS and utilizes cloud technologies including Elasticsearch, micro services, Apache Spark and Elastic proxies. By bringing these technologies together we have been able to scale to a petabytes-scale SaaS pipeline.

6.1.12. 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.

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Details on AWS data center controls: <https://aws.amazon.com/compliance/data-center/controls/>

Additionally, Tenable employs a Site Reliability Engineering team tasked with monitoring and oversight of the Tenable SaaS environment; as well as using tools to proactively monitor said environment. Tenable also deploys their management plain to multiple AWS to prevent outages to customer environments.

6.1.13. Ease of Use

The Solution shall be easy to use and configure, with an intuitive graphical user interface and clear documentation and support resources which instruct on use of the Solution.

This is a standard feature out of the box.

An intuitive GUI with advanced visualization and mapping tools gives you full situational awareness of your environment on a single pane of glass. Dashboard components have a variety of shapes and styles, including bar, pie, and matrices.

The product has context sensitive help and prompts to guide users in the use of the Solution, as well as full access to product guide documents, the Tenable Community site that provides both Tenable and peer product assistance.

6.1.14. Configuration Tools and Customization

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

Tenable.io enables customers to create their own custom dashboards, including visuals, tables and charts. Tenable offers a large number of dashboard templates out of the box at no additional charge and we have a dedicated team that creates new dashboards every week. These new dashboard and report templates are downloaded daily as part of the regular updates and customers can immediately use them. These dashboards are customizable and filterable by many attributes and can be drilled down into.

Tenable also has a Professional Services Team available to create custom dashboards.

6.1.15. Data Migration Services

The Solution shall provide data migration services to ensure a smooth transition of data from a Customer or Purchaser's current system to the Contractor's Solution.

6.1.16. Disaster Recovery Services

In the event of a disaster or system failure, the Solution shall provide disaster recovery services, including backup and a disaster recovery plan ensuring business continuity.

Tenable has disaster recovery and continuity procedures designed to help respond to situations that could occur and continue required business operations including Tenable.io. Business units have been provided recovery and resumption guidance. All systems are designed to be restored to a secondary site within 24 hours with a loss of at most the 2 hours of transient data (for scans in progress). Recovery exercises were completed per last requests to restore data.

Tenable.io is a cloud based service that operates on amazon web services (AWS). Physical security and maintenance are deferred to AWS policy for disaster recovery. Tenable.io has its own disaster recovery plan that helps respond to situations where business operations may be impacted. Tenable conducts business impact assessments to determine critical processes, dependencies, threats, impacts and figures out the recovery point objective and the recovery time objective.

Each data region has a specified DR replication site where we keep a "near-time" backup replica of data. The replica sites are encrypted with the same methods as the source sites and exist physically near the source site to reduce latency during fail-over operations as well as to maintain the physical sovereignty of the data.

Our business continuity policy and disaster recovery plan are tested annually.

6.1.17. Role-Based Access

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

Tenable.io RBAC settings support predefined groups, set by the customer. Role-Based Access Control (RBAC) allows users to have varying access to Tenable.io and permissions can be set as to which scans and reports users can access. Tenable.io RBAC settings support predefined groups, with permissions being set by the customer administrator directly within the application. RBAC can be used to create different groups to provide need-to-know separation of scan capability and the ability to view scan

results for different groups, and also grant access on an Asset which can contain a single or multiple IP addresses and/or subnets.

6.1.18. 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.

Tenable.io provides customers with the option to export data from nearly all dashboards into multiple formats according to their need. This data can be filtered on a plethora of fields, including assets, services, findings and more.

6.1.19. Integration

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

Tenable's technology integrations are continually expanding, and we have a large suite of possibilities. Tenable has integrations with a variety of Security and IT Operations technology partners as part of its Cyber Exposure ecosystem. Tenable alongside its ecosystem partners creates the world's richest set of Cyber Exposure data to analyze, gain context and take decisive action to better understand and reduce cyber risk. There are two ways to integrate with other tools:

Specific Partner Relationships: Tenable has pre-built integrations for several vendors and our integration list is continually expanding. Tenable's growing list of out-of-the-box integrations includes ServiceNow, CyberArk, Thycotic, Splunk, ForeScout, and many others. For a full list of integration partners, please visit: <https://www.tenable.com/integrations>

Out of the box open API: Tenable's products also include, at no additional charge, a RESTful API which allows for flexible integration with other tools. RESTful API is for developers who want to integrate Tenable's products with other standalone or web applications, and administrators who want to script interactions with the management console. The API is designed to allow automation to solve the same business problems that are solved via UI interaction. There are no technical limitations on the software on the rate and quantity of API usage.

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

Tenable.io can do this.

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

Tenable.io can do this.

6.1.19.4. Initial integration shall include connecting a Customer, upon request, to the State Cybersecurity Operations Center (CSOC) and validating with FL[DS] that all Solution data is properly integrated.

Tenable.io can do this.

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

Tenable.io can do this.

6.1.20. Performance and Availability

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

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

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Details on AWS data center controls: <https://aws.amazon.com/compliance/data-center/controls/>

Additionally, Tenable employs a Site Reliability Engineering team tasked with monitoring and oversight of the Tenable SaaS environment; as well as using tools to proactively monitor said environment. Tenable also deploys their management plain to multiple AWS to prevent outages to customer environments.

6.1.20.2. The Contractor 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.

WWT, Tenable and Foresite accept and will adhere to the SLA consequences listed in Table 1 within RFQ DMS-22/23-154.

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

WWT, Tenable and Foresite accept and will adhere to the SLA consequences listed in Table 1 within RFQ DMS-22/23-154.

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).

Tenable.io Introduction

The Tenable.io® Introduction Course is available for no cost at Tenable University and consists of a series of short on-demand videos providing the fundamental building blocks to deploy, configure and operate Tenable's cloud-based solution for vulnerability management. Tenable highly recommends this course as a prerequisite for the instructor-led Tenable.io Specialist Course. Participants in this course will learn how to install, configure and use the Tenable.io platform. Content includes asset discovery, vulnerability and compliance assessment, analysis of scan results, use of workbenches and dashboards, and how to

accept and recast risk. Tenable presents basic features and demonstrates usage for each topic.

Audience

This course is suitable for people interested in learning basic operational use of Tenable.io.

Prerequisites

None.

Course Syllabus

1. Introduction

- What is Cyber Exposure?
- The Cyber Exposure Lifecycle
- Tenable.io Capabilities
- Licensing

2. Installation and Configuration

- Tenable.io Sensors
- Nessus® Deployment
- Nessus Network Monitor (NNM) Deployment
- Tenable Core
- Scanner Groups
- User Management

3. Assessment

- Discovery Scan
- Intro to Vulnerability Assessment
- Non-Credentialed Assessment

4. Assessment, continued

- Credential Management
- Credentialed Assessment
- Compliance Overview
- Compliance Assessment
- Exclusions

5. Analysis

- Tagging
- Scan Analysis
- Compliance Analysis
- NNM Sensor Analysis
- Asset Workbench
- Vulnerability Workbench
- Dashboards
- Accepting and Recasting Risk

6. Tenable® Lumin

Tenable.io Specialist Course

This fast-paced Tenable.io® Specialist Course will give participants the knowledge and skills needed to effectively utilize Tenable.io, our cloud-based vulnerability management solution. It is designed for personnel responsible for identifying, investigating and remediating vulnerabilities and misconfigurations in their business environment.

This is a two-day course that is scheduled via the Tenable University once purchased. Users may sign up for any of the next available course as this one is instructor-led.

Overview

Participants in this two-day course will learn how to implement and support the Tenable.io platform. Content for the instructor-led course includes installation and configuration of Tenable.io, a review of Tenable.io operations, a technology overview along with architecture and design discussions for typical environments and a detailed scanning and analysis review.

Audience

This course is suited for professionals with operational responsibilities using Tenable.io who want to expand their knowledge to maximize the solution's effectiveness. It is recommended for those seeking to obtain Tenable.io Specialist Certification.

Prerequisites

Tenable highly recommends that all participants complete the free Tenable.io Introduction Course available at Tenable University before attending this course.

Course Syllabus

- | | |
|-------------------------------|--|
| 1. Welcome to Tenable | 8. Custom Dashboards |
| 2. Lab Environment | 9. Tenable Core |
| 3. Host Discovery | 10. Nessus® Installation |
| 4. Alternative Host Discovery | 11. Nessus® Network Monitor Installation |
| 5. Vulnerability Assessment | 12. Agents |
| 6. Compliance Assessment | 13. Scanner Groups and Networks |
| 7. Prioritization | 14. Role-Based Access Control |

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

This implementation schedule can be adjusted to suit the needs of Florida Digital Service (FL[DS]) and the entities participating in the cyber program.

Team Definitions	
Teams Defined	FL[DS] Service Experience Team FL[DS] Cyber Operations Team Tenable Sales Tenable TAM WWT Sales WWT Program Management Foresite Team
Groups Defined	<p>Pre-Sales Team:</p> <ul style="list-style-type: none"> • FL[DS] Service Experience Team • WWT Sales • Tenable Sales <p>Implementation Team:</p> <ul style="list-style-type: none"> • FL[DS] Service Experience Team • WWT Sales • Tenable Sales • WWT Implementation Team <p>Post Implementation Team:</p> <ul style="list-style-type: none"> • FL[DS] Service Experience Team • WWT Sales • Tenable Sales • Foresite Team

Pre-Implementation Activities

The following is a list of common activities that occur prior to implementation.

Pre-Implementation Activities and Tasks		
Demonstrations	Introduction to the solution: <ul style="list-style-type: none"> • Demonstrations to drive interest. • Technical Q&A sessions to provide answers to any outstanding questions. 	Lead: <ul style="list-style-type: none"> • FL[DS] Service Experience Team • WWT Sales • Tenable Sales
FL[DS] Questionnaire	Review and complete the FL[DS] questionnaire	Lead: <ul style="list-style-type: none"> • FL[DS]
	Review completed questionnaire and mark agency as "READY"	Lead: <ul style="list-style-type: none"> • FL[DS] Service Experience Team

The following is a list of common activities that occur during implementation. Agendas for calls and working sessions will include overviews and technical objectives for a given session. These agendas will be maintained throughout the program and include any lessons learned and updates to how the solution is deployed.

Implementation Activities and Tasks		
Call Schedule	Schedule a series of calls for implementation	Lead: <ul style="list-style-type: none"> • FL[DS] Service Experience Team Include: <ul style="list-style-type: none"> • WWT PM
Day 1 - Implementation Estimated Duration: 1 Day	Walk through implementation steps: <ol style="list-style-type: none"> Configuration Needs <ol style="list-style-type: none"> Review FW rules, AV exclusions, others Change Management process Key Agency Contacts (see examples below) <ol style="list-style-type: none"> SSO Administrator FW Administrator Security Administrator Deployment schedule small test group, larger test group, full roll out 	Lead: <ul style="list-style-type: none"> • Tenable Implementation Team Include: <ul style="list-style-type: none"> • WWT PM Foresite Team • FL[DS] Service Experience Team
Day 2 - Implementation Estimated Duration: 1 Day	Configure and Troubleshoot Tenable, if necessary	Lead: <ul style="list-style-type: none"> • Tenable Implementation Team Include: <ul style="list-style-type: none"> • WWT PM



		<ul style="list-style-type: none"> • Tenable Implementation Team • FL[DS] Cyber Operations Team •
Turn Over to Managed Services Estimated Duration: As Needed	Additional Configuration by Managed Services team to include additional networks, tags, users, compliance scans, and reports.	Lead: <ul style="list-style-type: none"> • Foresite Team Include: <ul style="list-style-type: none"> • FL[DS] Service Experience Team

Implementation Activities and Tasks		
Individual Agency Calls Estimated Duration: 30 - 60 Minutes	Per agency value calls	Lead: <ul style="list-style-type: none"> • FL[DS] Services Experience Include: <ul style="list-style-type: none"> • WWT Sales • Tenable Sales • Foresite Team

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

Internal asset inventory and discovery is not an MDR function. This section is not applicable to this RFQ response. However, we are responding within RFQ DMS-22-23-155.

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

Given the potential for dozens or hundreds of potential integration combinations, each with its own level of effort required to successfully complete the integration, WWT has developed a three-tier service delivery model based upon the forecasted level of effort with each use-case. This approach will result in a lower cost of delivery for the bulk of integration engagements.

Out-of-the-Box Integrations

Many solutions and products have built-in integration software that allows seamless integration between product 'X' and products 'A', 'B', and 'C'. Many require little more than sharing of an API authentication and/or encryption key between the two integration parties and configuration changes to each integration party, followed by validation testing and verification. It is likely that this mode of integration will represent the bulk of integration requirements.

Custom Integrations – Simple

Some products and solutions may require the development of custom plugins, utilizing a common Application Programming Interface (API) to accomplish an integration with a third-party solution. In the use case where out-of-the-box integration is not possible but each integration component supports

standard RESTful APIs, WWT will deliver the integration service to include all API calls necessary to support the desired integration.

Custom Integrations – Complex

In rare cases, there may exist a desire to integrate multiple solutions which have no obvious and/or direct manner with which to integrate. In these use-cases, WWT will, within the boundaries of possible and avoiding actions which may violate the terms & conditions of the End User Licensing Agreement (EULA), develop a mechanism whereby previously unsupported integrations are delivered. WWT personnel will deliver the software (scripts, API calls, source-code, etc.) necessary to enable the specifically defined capabilities of the customer. This will not be a common occurrence.

The below pricing table is Not-to-Exceed (NTE) pricing. Any integrations will need to be scoped and a firm fixed price or billable hours statement of work can be created for each integration. All hours and pricing are estimates provided in the table below.

Integration Type	SLA Integration Timeline	Estimated Hours	Estimated Pricing	Resources
Out of the box integrations	1 week	48 hours	\$15,500	Solutions SME/Project Manager
Custom Integrations – Simple	4 weeks	192 hours	\$61,500	Solution SMEs/Application Developers/Project Manager
Custom Integrations – Complex	8 weeks	384 hours	\$123,000	Solution SMEs/Application Developers/Project Manager

Assumptions:

- RESTful APIs or modern API should be available for integration
- Solutions involved in integrations should be still supported by the vendor
- A scoping session will need to be held to discuss the integration and use cases to be addressed with the integration to set specific integration delivery timeline
- A combination of Solutions SMEs, Project Manager, and Application Developers will work together to develop and enable these integrations depending on scoping conversations with the customer
- If an integration does not seem viable after the scoping session for technical or business reasons, WWT will discuss alternatives to meet the use cases detailed for this integration
- If scoping determines the integration effort is greater than eight weeks, a custom statement of work will be required.

f. A draft disaster recovery plan per section 30.5.

Foresite Cybersecurity's ProVision platform prioritizes reliable service with a comprehensive Disaster Recovery Plan (DRP). This plan includes a proactive structure identifying key personnel and their responsibilities, ensuring rapid response during a crisis. It covers contingencies for a range of incidents, from minor system failures to major natural disasters. The Business Continuity Team and IT Recovery Team work together to manage the recovery process, from strategic planning to the rapid restoration of IT systems. Regular audits, tests, and updates are conducted to maintain the plan's effectiveness. With Foresite, customers are assured of a resilient, protected service that anticipates and prepares for potential threats.

The Foresite ProVision platform is cloud based (Amazon AWS) with multiple availability zones and multiple Security Operations Centers (SOCs) in the United States. Their engineers and analysts can also work remotely as the final option using our Cloud based platform.

ProVision Platform

Foresite has developed their own proprietary multi-tenant Managed Security Services Platform, ProVision, and has all the design, development, and implementation resources in-house. The solution infrastructure is hosted on AWS, giving the platform the scalability, flexibility, and performance to exceed the needs of the State of Florida's customer base. They can also tailor requirements to specific customer or project needs as they own all the code and resources.

ProVision delivers real-time analysis of security events generated across a customer's entire infrastructure. ProVision handles log storage and management, correlation of events through advanced analytics and machine learning and application of security intelligence feeds. Foresite's SOC teams provide additional event enrichment for identification, assessment, notification, and escalation. Other services in the ProVision suite include **Device Management** where they manage or co-manage a customer's security infrastructure; **Patch Management** to ensure the customer is systematically keeping up to date with operating system and application updates; **Managed Detection and Response (MDR)** where Foresite is actively hunting for threats across the customer environment; **Security Testing** such as Penetration Testing, Application Testing, Phishing Campaigns, Red/Blue/Purple Teaming, Code Review, Site Surveys and more; plus a host of **Security Consultancy** such as helping customers achieve ISO 27001 certification, Cyber Essentials +, PCI Gap Analysis, Cloud Security Posture, vCISO and more.

Foresite has been active as a Managed Security Service Provider (MSSP) since 2014. Several of the leaders in their organization previously built an earlier iteration of an MSSP and brought many key learnings forward to Foresite. The services they deliver are critical in helping customers who are typically understaffed, overwhelmed and lacking in broad security know-how. Foresite does not resell product but is vendor agnostic. They have a very specific focus around MSSP, Compliance and Security Consulting Services.

Foresite's target market is the small and medium-sized enterprises (SME) space. They pride themselves in delivering a customer experience to SME customers that is best of class among MSSPs. Foresite's customer retention rate in the SME market is 95+%. Customers frequently laud their proactive engagement with their teams, ProVision's ease of use and the quality of their personnel.

Foresite is ISO:27001 certified and the datacenter is SOC 1&2 compliant.

ProVision Security Services Suite

MDR- Managed Detection Response

Active Threat Hunting to identify potential areas of compromise including detection, analysis, response and remediation. Providing outcomes - not alarms - with faster Incident Response times and working as an extension of your Security Team

Patch Management

Full unified patching across the organization securing all the end-points and infrastructure in your network. Evaluate, Test and apply operating system and application patches automatically as a service.

SOG-as-a-Service

Defend against advanced and complex security threats with a 24x7x365 cyber security center providing all your security services requirements.

Consulting & Compliance Solutions

Gap assessments, certified audits/attestations (PCI, ISO 27001, Cyber Essentials +, more.),

Security Testing & Assessment

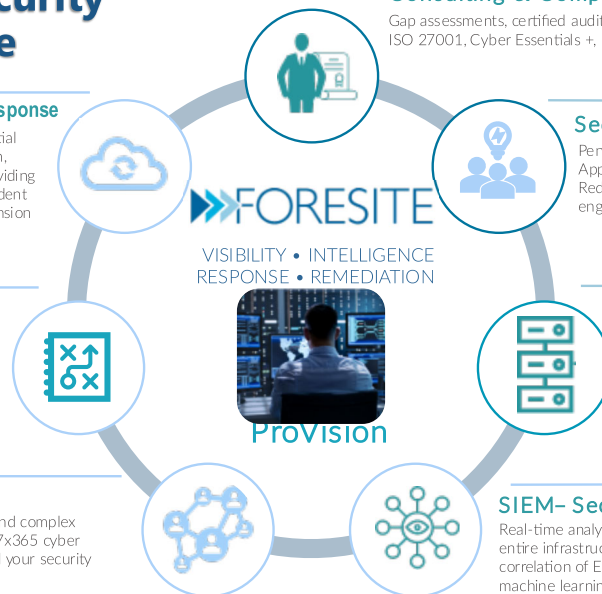
Penetration Testing, Vulnerability Assessment, Application Testing, Social Engineering, Phishing, Red Team Testing and more. Individual engagements or Service Schedules.

Critical Asset Mgt

Firewall / End-point / O365 (& more) Monitoring & Management with 24x7x365 access to skilled Security Experts as an extension of your Security Team. Full incident analysis, remediation, change control and system updates/upgrades.

SIEM- Security Monitoring

Real-time analysis of Security Events generated across the entire infrastructure. Log storage & management, correlation of Events through advanced analytics and machine learning, combined with Security Intelligence feeds and human enrichment for identification, assessment, notification and escalation.



5

Tenable ASM

Tenable Disaster Recovery Plan Summary

From a high level, the Bit Discovery DR plan is based on a backup and restore recovery procedure. Periodic backups of its main DB as well as required caches will ensure that IT operators can quickly bring systems back online to meet tier 1 RTO. The plan described is structured such that after executing Tier1, Bit Discovery will be in compliance with its customer SLAs.

Tier 2 largely aims to stay true to Bit Discovery's data-freshness SLAs and will have RTOs associated with them. Tier 3 will largely address recovery of backend data-pathways and internal systems to bring all systems up to 100% functionality. At this point Bit Discovery may choose to fail back or continue at the failover site. In either case it'll need to re-establish redundancy by implementing backups at a designated failover Region at that point in time.

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

Foresite Cybersecurity has been performing external, internal, wireless and physical network security scanning and testing for more than 10 years. On average, they perform 250 engagements per year for scanning and testing services.

Tenable reference customers are available upon request.

<https://www.tenable.com/case-studies/public-sector-organisation>

<https://www.tenable.com/case-studies/a-government-health-agency>

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

Foresite Cybersecurity has been performing external, internal, wireless and physical network security scanning and testing for more than 10 years. On average, they perform 250 engagements per year for scanning and testing services.

Tenable has the ability to do global implementations. For 23 years, we have provided professional services to implement our solutions both remote and onsite. We perform thousands of quick starts yearly both onsite and remote. Examples available upon request with permission from customers.

4) Document any substantial deviations within Vendor's Solution from the Scope of Work.

There are no substantial deviations within our solution from the Scope of Work.

5) Detail regarding any value-added services.

In a challenging world where the landscape has changed and attacks are increasing, WWT looks forward to speaking with the State of Florida about how we can assist with our people, our labs and our WWT Digital Platform. Our Cyber Security Project Team has been built to help drive the Department's security program and business outcomes with our security services, Strategic Staffing capabilities, and the proactively offered resources behind them to that bring education, insight and depth to the State of Florida team.

World Wide Technology's Value Added-Service

Advanced Technology Center (ATC)

To answer the most complex questions, we have developed an immersive learning platform, powered by our ATC and designed to be at the forefront of what is possible. This physical and virtual ecosystem of innovation, research, community, labs and thought leadership accelerates the Department's knowledge in cybersecurity.

The ATC is a collaborative ecosystem used to design, build, educate, demonstrate and deploy innovative technology products and integrated architectural solutions for our customers, partners and employees around the globe. The heart of the ATC is our Data Centers which house 500+ racks of equipment used to cut technology evaluation time from months to weeks, if not days.

We partner with the world's leading technology manufacturers — from Silicon Valley heavyweights to emerging tech players — to deliver innovative solutions that drive business outcomes and position our customers to take on the business challenges of tomorrow.

Adopting a combination of on-premise, off-premise and public cloud capabilities is the only way to keep up with the rapid market changes digital disruption is driving. The ATC is a replica of that ever-changing landscape with integration into all three major Cloud Service Providers, leveraging low latency connections through our Equinix Extension as shown in Figure 1.

We use enterprise-class traffic generation tools, such as Ixia IxLoad, to simulate the applications that are unique to the Department to show how a solution seamlessly integrates into its network. Over the years, WWT has developed a testing framework that allows us to go from concept to test plan to achieve the outcome needed for product or solution evaluation. This yields the following benefits:

- Testing use cases
- Comparison
- Upgrade/Migration
- Architecture Validation
- Performance
- Functionality



Figure 1

The ATC infrastructure facilitates fast proofs of concept for current and future use cases.

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

Please see Attachment A, Price Sheet included with our submission.

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

Please see Attachment B, Contact Information Sheet included with our submission.

8) Non-Disclosure Agreement executed by the vendor.

Please see executed Non-Disclosure Agreement included with our submission.

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.

World Wide Technology

In a challenging world where the landscape has changed and attacks are increasing, WWT looks forward to speaking with the State of Florida about how we can assist with our people, our labs and our WWT Digital Platform. Our Cyber Security Project Team has been built to help drive the Department's security program and business outcomes with our security services, Strategic Staffing capabilities, and the proactively offered resources behind them to that bring education, insight and depth to the State of Florida team.

Advanced Technology Center (ATC)

To answer the most complex questions, we have developed an immersive learning platform, powered by our ATC and designed to be at the forefront of what is possible. This physical and virtual ecosystem of innovation, research, community, labs and thought leadership accelerates the Department's knowledge in cybersecurity.

The ATC is a collaborative ecosystem used to design, build, educate, demonstrate and deploy innovative technology products and integrated architectural solutions for our customers, partners and employees around the globe. The heart of the ATC is our Data Centers which house 500+ racks of equipment used to cut technology evaluation time from months to weeks, if not days.

We partner with the world's leading technology manufacturers — from Silicon Valley heavyweights to emerging tech players — to deliver innovative solutions that drive business outcomes and position our customers to take on the business challenges of tomorrow.



Figure 1
The ATC infrastructure facilitates fast proofs of concept for current and future use cases

Adopting a combination of on-premise, off-premise and public cloud capabilities is the only way to keep up with the rapid market changes digital disruption is driving. The ATC is a replica of that ever-changing landscape with integration into all three major Cloud Service Providers, leveraging low latency connections through our Equinix Extension as shown in Figure 1.

We use enterprise-class traffic generation tools, such as Ixia IxLoad, to simulate the applications that are unique to the Department to show how a solution seamlessly integrates into its network. Over the years, WWT has developed a testing framework that allows us to go from concept to test plan to achieve the outcome needed for product or solution evaluation. This yields the following benefits:

- Testing use cases
- Comparison
- Upgrade/Migration
- Architecture Validation
- Performance
- Functionality

WWT Cyber Range

WWT Cyber Range, formerly called Lab as a Service, addresses the need for our customers to upskill their staff, compare and test new technologies and configuration changes, gain insights into industry innovation, and accelerate successful adoption in a safe and secure environment. WWT offers a free monthly Cyber Range where your teams can join and sharpen their security skills in our environment competing against other teams from around the world.

WWT's Cyber Range provides operations teams unprecedented training and access to a suite of commercial tools that are actually used in a real-world cyber incident. Customers can also leverage

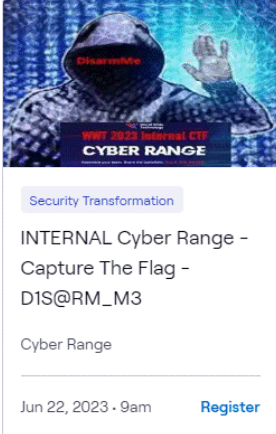
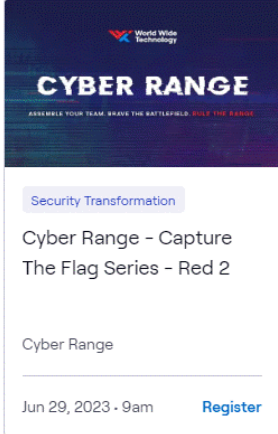
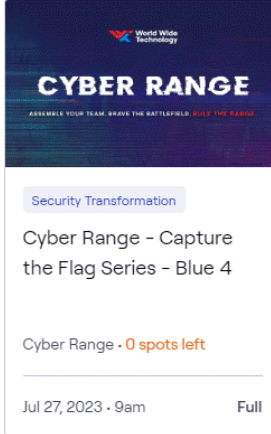
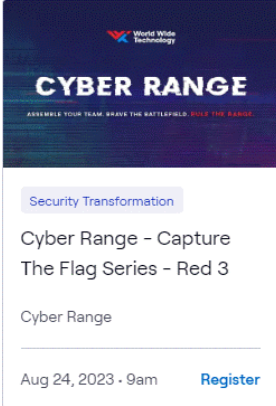
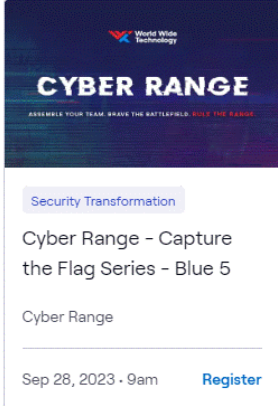
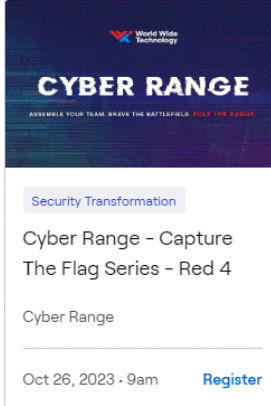
The State of Florida Department of Management Services
May 2023



WWT's Advanced Technology Center (ATC) support staff, and our expansive list of OEM partnerships, to build their own customized cyber range environment to suit their unique needs.

In a world with ever-evolving security threats, the need for comprehensive security solutions has never been greater. WWT's Cyber Range is a virtual arena to fortify your cyber defenses across your people, process and technology.

Upcoming Capture The Flag events:

 <p>Security Transformation</p> <p>INTERNAL Cyber Range - Capture The Flag - DIS@RM_M3</p> <p>Cyber Range</p> <p>Jun 22, 2023 - 9am Register</p>	 <p>Security Transformation</p> <p>Cyber Range - Capture The Flag Series - Red 2</p> <p>Cyber Range</p> <p>Jun 29, 2023 - 9am Register</p>	 <p>Security Transformation</p> <p>Cyber Range - Capture the Flag Series - Blue 4</p> <p>Cyber Range - 0 spots left</p> <p>Jul 27, 2023 - 9am Full</p>
 <p>Security Transformation</p> <p>Cyber Range - Capture The Flag Series - Red 3</p> <p>Cyber Range</p> <p>Aug 24, 2023 - 9am Register</p>	 <p>Security Transformation</p> <p>Cyber Range - Capture the Flag Series - Blue 5</p> <p>Cyber Range</p> <p>Sep 28, 2023 - 9am Register</p>	 <p>Security Transformation</p> <p>Cyber Range - Capture The Flag Series - Red 4</p> <p>Cyber Range</p> <p>Oct 26, 2023 - 9am Register</p>

Use WWT's Cyber Range to:



Accelerate evaluation of advanced cyber technologies that boost resiliency. Risk reduction and value realization through hands-on testing and exposure to the latest innovations in cybersecurity.



Bolster your capabilities by enhancing skillsets for emerging tools and solutions. Real-world training to sharpen your teams' cybersecurity skills and increase vigilance in an ever-evolving threat landscape.



Strengthen your posture by assessing individual skills and identifying gaps on your teams. Get hands-on with new attacks and vulnerabilities to evaluate how your defenses stack up to industry benchmarks.

Cyber Range is powered by the WWT ATC

WWT's Advanced Technology Center (ATC) Platform is a capability that organizations can lean on to make smart technology decisions fast to accelerate security transformation.

There is no other platform in the world that features:

- Insight and intellectual capital that reaches into every sector of the economy
- Industry-leading partnerships with the world's largest OEMs and technology companies
- Independent and informed guidance with a customer-centric approach

Use our platform to:










- Get hands-on, on-demand experience
- Capture real-world insights and research
- Leverage practical and actionable guidance
- Compare, contrast and validate multi-vendor solutions
- Think creatively about strategy
- Tap into our industry-leading expertise and unparalleled training

WWT Digital Platform @ <https://www.wwt.com>

WWT customers have access to the WWT Platform @ <https://www.wwt.com> which is a educational and training platform with deep technical content on technology solutions and business that can help drive your business outcomes. From insight articles on Security Transformation to updates on the partners ecosystem, this is a rich resource for all of your team from executives to security analysts. This is where we host our industry leading articles, labs, and communities to educate and collaborate with our customers, partners and colleagues.

WWT Free Training on the WWT Platform

WWT has free training thru our WWT Learning Paths on the WWT Platform that all customers can utilize. There are currently over 22 current Learning paths around Technology and Security Solutions from Identity & Access Management to Data Protection to DevOps to AWS and more. Below is a sample of the free training courses available.

<p>BETA</p> <p>Identity & Access Management with CyberArk</p> <p>Identity & Access Management with CyberArk</p> <p>Learning Path  Fundamentals</p> <p>~5 hrs View Path</p>	<p>BETA</p> <p>Cisco ACI Fundamentals</p> <p>Cisco ACI Fundamentals</p> <p>Learning Path  Fundamentals</p> <p>~13 hrs View Path</p>	<p>BETA</p> <p>DevOps Principles</p> <p>DevOps Principles</p> <p>Learning Path  Fundamentals</p> <p>~3 hrs View Path</p>
<p>BETA</p> <p>Collaboration System Release 12.5</p> <p>Collaboration System Release 12.5</p> <p>Learning Path  Fundamentals</p> <p>~17 hrs View Path</p>	<p>BETA</p> <p>Application Delivery Controller Foundations</p> <p>Application Delivery Controller Foundations</p> <p>Learning Path  Fundamentals</p> <p>~1 hr View Path</p>	<p>BETA</p> <p>SD-Branch with Juniper</p> <p>SD-Branch with Juniper</p> <p>Learning Path  Fundamentals</p> <p>~1 hr View Path</p>
<p>BETA</p> <p>Collaboration System Release 14</p> <p>Collaboration System Release 14</p> <p>Learning Path  Fundamentals</p> <p>~17 hrs View Path</p>	<p>BETA</p> <p>Fortinet FortiVoice</p> <p>Fortinet FortiVoice</p> <p>Learning Path  Fundamentals</p> <p>~1 hr View Path</p>	<p>BETA</p> <p>Rubrik Data Protection Fundamentals</p> <p>Rubrik Data Protection Fundamentals</p> <p>Learning Path  Fundamentals</p> <p>~5 hrs View Path</p>

WWT Security Transformation Briefings

WWT will host routine Security Transformation briefings on a monthly and quarterly basis to give knowledge and insights on specific security topics to increase the security awareness and security maturity of all organizations.

WWT State-wide CISO roundtable

WWT will host a State-Wide CISO roundtable for CISOs and security executives across the State where we will dive into security topics and provide access to our WWT Security Experts. This interactive

roundtable will allow security knowledge sharing and collaboration amongst all of the State-wide CISOs, WWT Security Experts and security executives to drive security maturity of all organizations.

Some topics that can be topics of these sessions are:

- Explore and simplify hot security topics
- Process Challenges
- Transforming your security architecture and responding to the needs of the business require seamless operations, cross- functional alignment and big picture planning.
- Segmentation Strategy
- MRA Remediation
- Security Transformation: Successful outcomes leveraging ATC & Cyber Range as a Service
- Transformational Security Buying, Rationalization
- Convergence of network and security services (SASE)
- Break down silos in SecOps solution stack (XDR)
- Operational shift toward zero trust maturity (ZTA)
- Maintain compliance and enforce security across multicloud
- Prune and optimize observability pipeline for security
- Simplify identity management and adopt passwordless

WWT Security Assessments

WWT will host security assessments on a routine basis in a workshop format to drive security outcomes. WWT's Security Assessments are for Department-identified security and operation teams and other key stakeholders. Our subject matter experts provide a customized assessment that enables the Department to understand emerging threats and develop a security strategy for increasing its security maturity for people, process and tools.

After conducting the assessment, WWT can offer the Department access to our ATC to further evaluate endpoint security solutions through a hands-on, practical approach. This includes customized product demos, real-world solution comparisons and integrations with our Cyber Analytics Reference Architecture, which includes SIEMs, automation and orchestration.

WWT Security Community Page and “Hour of Cyber”

WWT will host a security community page for the Department and its customers to drive security collaboration and content. Videos and content can be posted here for internal training and knowledge sharing among the Department and its customers.

We live in a time of extremes — on one end is cyber disruption, on the other, rapid innovation. WWT recognizes how important it is for security leaders to have a safe space for curated focused discussions from both business and technical perspectives.

Foci of this security community and “Hour of Cyber” are:

- Explore and simplify hot security topics
- Conquer the speed and complexity of cyber threats
- Share challenges faced by other global organizations
- Chart a path toward security transformation
- Capture and prioritize concerns and challenges
- Develop a plan to drive outcomes and fulfill business needs

What is “Hour of Cyber?”

Our goal is to focus on the Department’s particular security needs and create a plan for a successful, optimized security transformation strategy. Sessions are scheduled for 50 minutes total, with 20 minutes for thought leadership exploration and 30-minutes for interactive dialogue and discussion.

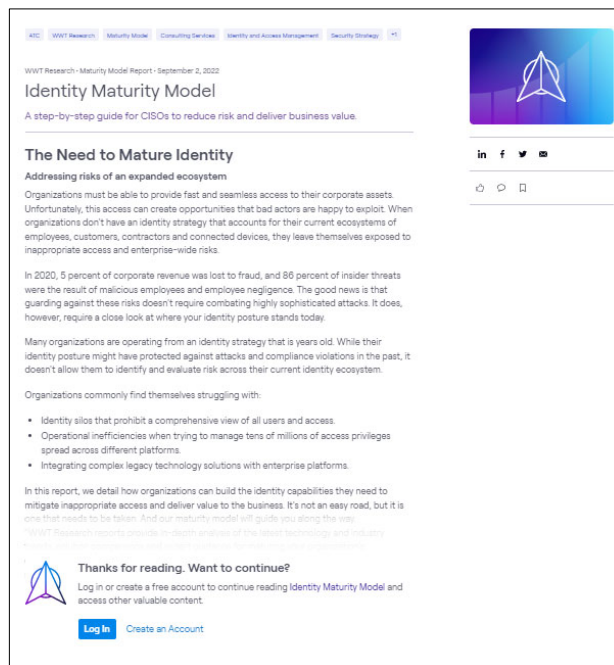
WWT Community Example Link

This is a WWT Community that we created for the State of Florida Tanium project. It can be accessed through the link below to see an example of a WWT Community and its content.

<https://www.wwt.com/community/wwt-florida-digital-services-tanium-services-project/about>

WWT Research

WWT Research Reports gives insights as thought leaders in the market. Our **Technology Evaluations, Maturity Models, Priorities Reports, and Artificial Intelligence and Machine Learning (AI/ML) Applied Research Reports** each provide compelling business and technology insights that help the Department make smarter technology decisions faster and imagine the art of the possible. The screenshot below reveals a typical format for our WWT Research Reports.



These reports provide actionable insights into technology solutions and trends that can help you make more informed decisions and outpace the competition. Please see the links below for two WWT Research Reports.



Security Priorities for 2023 [Explore](#)



Security Maturity Model [Explore](#)

WWT TEC37 Podcasts

WWT hosts monthly technical webcasts on different security and technology topics that are available for our customers. We all learn differently. That's why we dive deep into security and technology on WWT TEC37 Podcasts through conversations with our experts. Please follow the links below for the podcasts.



[Network Security](#)
[Securing and Scaling a Workforce On-the-Go with SASE | Research](#)
Webinar



[Security Transformation](#)
[Making Sense of Identity and Access Management | Research](#)
Webinar



[Security Transformation](#)
[Let Me Be Clear: How to Gain Clarity and Control to Bolster Your Cyber Defenses | Research](#)
Webinar



[Security Transformation](#)
[TEC37 Security Series E10: Five Essential Steps to Improve Security Maturity](#)
Webinar

WWT Case Studies

Our case studies show how we have helped organizations across industries adopt enterprise security programs that put the business first. Please follow the links below.



[Customer Experience](#)
[Building a Modern, Elastic IT Infrastructure From Scratch for Elanco Animal Health to Streamline and Optimize M&A](#)
Case Study



[Customer Experience](#)
[Creating the Perfect Pizza Kitchen for Little Caesars](#)
Case Study



[SASE](#)
[Global Pharmaceutical Company Accelerates Comparison of SASE Solutions](#)
Case Study



[Zero Trust](#)
[Manufacturer Establishes Micro-segmentation Strategy to Address Risks of Flat Network](#)
Case Study



[Campus & LAN Switching](#)
[Global Pharmaceutical Company: Software-Defined Access Deployment](#)

Case Study



[Cyber Resilience](#)
[Manufacturer Recovers From Costly Ransomware Attack](#)

Case Study

Foresite Cybersecurity

Managed Tenable.io

Tenable.io is a cloud-based vulnerability management solution developed by Tenable, a well-respected in the industry, vulnerability scanning company. Its primary function is to help organizations identify and remediate vulnerabilities in their infrastructure to enhance their security posture.

Here are some of the key features and functionalities of Tenable.io:

- **Vulnerability Management:** Tenable.io provides a robust and comprehensive vulnerability management solution. It can identify vulnerabilities in your network, applications, and even cloud infrastructure. This includes traditional IT assets, as well as modern assets like web applications, cloud instances, and containerized applications.
- **Predictive Prioritization:** Tenable.io uses machine learning to prioritize vulnerabilities based on the threat they pose to your organization. This allows you to focus your remediation efforts on the vulnerabilities that matter most.
- **Integration and API:** Tenable.io offers robust APIs and integration capabilities, allowing you to integrate it with your existing security and IT tools. This can help streamline your workflows and improve your overall security operations.
- **Compliance and Reporting:** Tenable.io can also help with compliance efforts. It can assess your infrastructure against various regulatory and industry standards and provide detailed reports to demonstrate compliance.

Deliverable	Description
Engagement Deliverable	Executive Summary: <ul style="list-style-type: none"> • High level presentation on assessment activities and results during QBR meetings.

	<ul style="list-style-type: none"> • A detailed report on findings on a monthly cadence. <p>Technical Summary:</p> <ul style="list-style-type: none"> • All systems in the data environment that are connected to the Internet and within the internal environment discovered in the course of the engagement. This will include all information discovered about those systems (i.e. operating systems, available services, version information.) • A prioritized list of vulnerabilities discovered and potential impact (if known) • Recommendations to improve information security posture.
--	---

Knowledge Transfer

Foresite encourages the involvement of our Customer's staff and will provide knowledge transfer as part of the engagement. Participation throughout the engagement is determined by Customer's availability.

Data Retention

Foresite will retain a copy of Reports and supporting Customer Data in accordance with Foresite's record retention policy (up to 1 year before secure destruction).

Foresite's ProVision Platform

Foresite have developed our own proprietary multi-tenant Managed Security Services Platform, ProVision, and have all the design, development, and implementation resources in-house. The solution infrastructure is hosted on AWS giving the platform the scalability, flexibility, and performance to exceed the needs of State of Florida's customer base. We can also tailor requirements to specific customer or project needs as we own all the code and resources.

ProVision delivers real-time analysis of security Events generated across the customer's entire infrastructure. ProVision handles log storage and management, correlation of events through advanced analytics and machine learning and application of security intelligence feeds. Our SOC teams provide additional event enrichment for identification, assessment, notification, and escalation.

Optional services in the ProVision suite include:

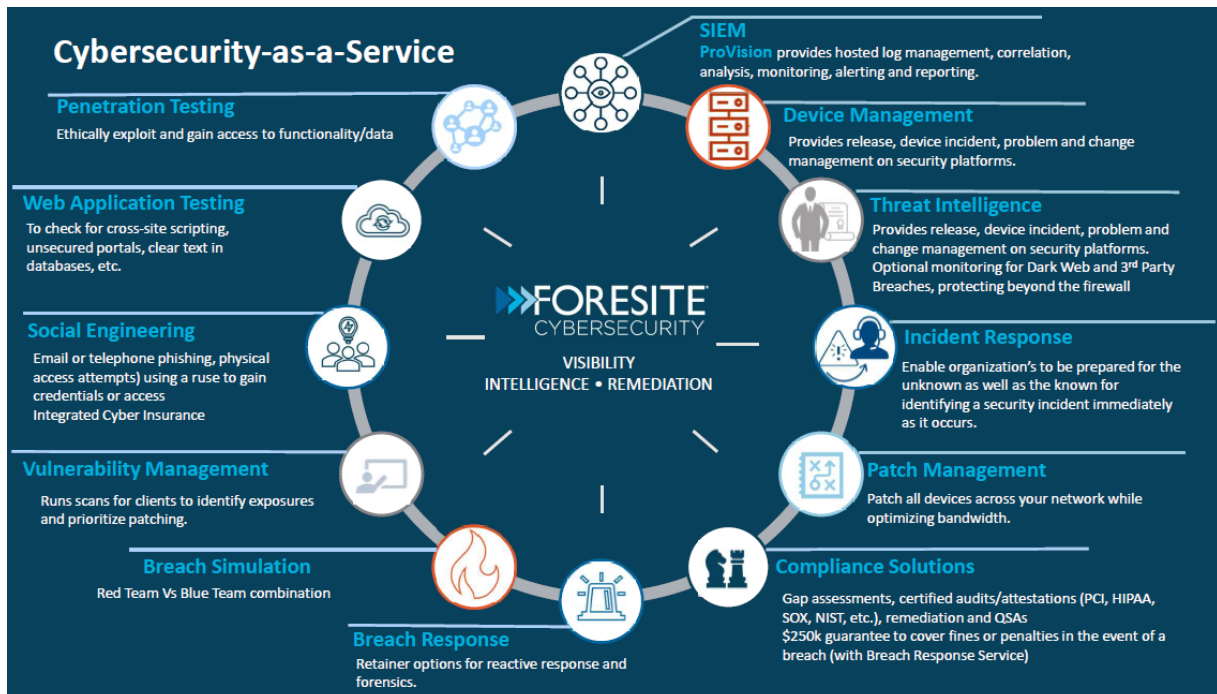
- **Device Management** where we manage or co-manage the customer's security infrastructure;
- **Patch Management** to ensure the customer is systematically keeping up to date with operating system and application updates;
- **Managed Detection and Response (MDR)** where we are actively hunting for threats across the customer environment;
- **Security Testing** such as Penetration Testing, Application Testing, Phishing Campaigns, Red/Blue/Purple Teaming, Code Review, Site Surveys and more; plus a host of
- **Security Consultancy** such as helping customers achieve ISO 27001 certification, Cyber Essentials +, PCI Gap Analysis, Cloud Security Posture, vCISO and more.

Foresite has been active as an MSSP since 2014. Several of the leaders in our organization previously built an earlier iteration of an MSSP and brought many key learnings forward to Foresite. The services we deliver are critical in helping our SME customers who are typically understaffed, overwhelmed, and

lacking in broad security know-how. Foresite doesn't resell product, we're vendor agnostic. We have a very specific focus around MSSP, Compliance and Security Consulting Services.

Our target market is the SME space. We pride ourselves in delivering a customer experience to our SME customers that is best of class among MSSPs. Our customer retention rate in the SME market is 95+%. Customers frequently laud our proactive engagement with their teams, ProVision's ease of use and the quality of our personnel.

Foresite is ISO:27001 certified and the datacentre is SOC 1&2 compliant.



Tenable Transfer of Licenses

Transferability of Licenses

Transfer of license between entities is a simple process with Tenable. A simple form must be completed and signed by the entity receiving the license and sending the license. This can be done with the Tenable Account Team.

Tenable Additional Support Options

The below speaks to the option higher level support that can be used at an additional cost.

Support Options

- Premier Support
- Elite Support

Premier Support Plan Features

Tenable Community

All named contacts with a valid support contract may open a support case by logging into the Tenable Community. The Tenable Community contains the Knowledge Base, documentation, and license information as well as the list of available phone numbers (for customers with phone support) and a

button to initiate a live chat session. The primary support contact may also add/remove support contacts using the Community.

Chat Support

Chat support is available to customers with Premier Support plans 24 hours a day, 365 days a year. The chat feature is available once a named contact has logged into the Tenable Community.

Phone Support

Phone support is available to named support contacts with Premier Support plans 24 hours a day, 365 days a year. Phone numbers are listed in the Tenable Community.

Direct Access to the Level 2 Support Engineer (TSE) team

The Level 2 TSEs are senior members of the Tenable Technical Support staff with deep technical experience with Tenable solutions.

The Level 2 Technical Support Engineers are globally based in the Tenable Technical Support offices and are available 24 hours a day.

The Department may designate up to 10 contacts who will have direct access to the Premier TSE team.

Summary of benefits:

- Bypass Level 1 support. Direct access to a Level 2 Senior Technical Support Engineer by phone.
- Supported completely by a team of Level 2 Senior TSEs with high level of professional and communication skills.
- Faster response and resolution times reflected in the lowered SLA Time Frames.
- Overall cases reduced due to experience and strength of troubleshooting work.

Support Contacts

An account is limited to ten (10) named support contacts who are authorized to contact Technical Support. Support contacts must be reasonably proficient in the use of information technology, the software they have purchased from Tenable, and familiar with the customer resources that are monitored by means of the software. Support contacts must speak English and conduct support requests in English. Support contacts must provide information reasonably requested by Tenable for the purpose of resolving a support request.

Elite Support Plan Features

Email Support

Email support is available to five (5) designated Elite support contacts who have direct access to their Elite Technical Support Engineer (TSE) during local/agreed business hours.

Tenable Community

All named contacts with a valid support contract may open a support case by logging into the Tenable Community. The Tenable Community contains the Knowledge Base, documentation, and license information as well as the list of available phone numbers (for customers with phone support) and a button to initiate a live chat session. The primary support contact may also add/remove support contacts using the Community.

Chat Support

Chat support is available to customers with Elite Support plans 24 hours a day, 365 days a year. The chat feature is available once a named contact has logged into the Tenable Community.

Phone Support

Phone support is available to five (5) designated Elite support contacts who have direct access to their Elite Technical Support Engineer (TSE) during local/agreed business hours. Non-named Elite support contacts can engage Tenable Advanced Support 24 hours a day, 365 days a year. Phone numbers are listed in the Tenable Community.

Direct Access to the Elite Technical Support Engineer (TSE) team

The Elite TSE is a senior member of the Tenable Technical Support staff with deep technical experience with Tenable solutions.

The Elite Technical Support Engineer is based in the Tenable Technical Support office closest to the customer and will be available from 9am - 5pm in the local time of that support office. Support outside of these hours will be handled by the first available senior engineer in the region.

Maryland, USA	9:00am to 5:00 PM
Dublin, Ireland	9:00am to 5:00 PM
Singapore, Singapore	9:00am to 5:00 PM

Customers may designate up to five (5) contacts who will have direct access to the Elite TSE team.

Summary of benefits:

- Bypass Level 1 support. Direct access to L2 Elite TSE support
- Intimate knowledge of customer environment, network topology, assets, deployment locations, deployment schedules
- Proactive support
- Holistic case management
- Early entry access to beta releases.
- Exclusive access to Technical Support tools & communities.

Support Contacts

An account is limited to ten (10) named support contacts who are authorized to contact Technical Support. Support contacts must be reasonably proficient in the use of information technology, the software they have purchased from Tenable, and familiar with the customer resources that are monitored by means of the software. Support contacts must speak English and conduct support requests in English. Support contacts must provide information reasonably requested by Tenable for the purpose of resolving a support request.

Pursuant to the terms and conditions of the RFQ, WWT shall conform to Section 22: Use of Subcontractors by having a contract with WWT's contractors, subcontractors, and subvendors providing for alternate the payment terms, as is permitted under per section 287.0585(2), F.S.

**ATTACHMENT A
PRICE SHEET**

I. Alternate Contract Source (ACS)

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

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

II. Pricing Instructions

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

III. Pricing

All below pricing is Not-To-Exceed (NTE) Pricing.

The **minimum** number of observable objects that must be purchased from a licensing, implementation and managed service point of view is sixty-five (65).

**Tenable.io with Implementation and Training
(Based on 100,000 Observable Objects)**

Initial Term Pricing (Years 1-3)		
Item No.	Description	Rate Per User (A)
1	<u>Initial Software Year</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include: <ul style="list-style-type: none"> • Implementation • initial training • Initial Integration • integration maintenance • support services 	\$ 7.84
2	<u>Subsequent Software Year</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include: <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ 2.63

(Optional) Renewal Term Pricing (Years 4-6)		
Item No.	Description	Rate Per User (A)
1	<u>Renewal Software Year (~15% increase from Year 1)</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include: <ul style="list-style-type: none"> • Implementation • initial training • Initial Integration • integration maintenance • support services 	\$ 9.02
2	<u>Subsequent Software Year (~5% YoY Increase)</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include: <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ 3.03

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
Tanium Waterfall Software SKUs			
TIOVM	Tenable.io Vulnerability Management Assets: 65 - 100,000 (Pricing Based on 100,000) - \$2.63 per object per year Term: 12 Months Tenable Public Sector LLC - TIOVM	\$ 314,090.00	\$ 263,484.20
TIOVM	Tenable.io Vulnerability Management Assets: 100,000+ (Pricing Based on 500,000) - \$2.40 per object per year Term: 12 Months Tenable Public Sector LLC - TIOVM	\$ 1,649,340.00	\$ 1,198,936.17
TIOVM-STNDC	Standard Tenable.io VM Container Term: 12 Months TENABLE.IO VM CONTAINER	\$ -	\$ -
World Wide Technology Implementation Services			
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Per Device	\$ 25,000.00	\$ 5.21

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
Tenable Waterfall Pricing			
TIOVM	Tenable.io Vulnerability Management Assets: 65 - 100,000 (Pricing Based on 100,000) - \$2.63 per object per year Term: 12 Months Tenable Public Sector LLC - TIOVM	\$ 314,090.00	\$ 263,484.20
TIOVM	Tenable.io Vulnerability Management Assets: 100,000+ (Pricing Based on 500,000) - \$2.40 per object per year Term: 12 Months Tenable Public Sector LLC - TIOVM	\$ 1,649,340.00	\$ 1,198,936.17

Item No. 3 – ACS Pricing Breakdown (Optional - But HIGHLY Recommended - Not included in Per Device Pricing)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
Tenable Training			
TRG-TIO-ESS-SEAT	2 Day Seat - Access for 1 person to attend an available session of Tenable.io Essentials	\$ 2,000.00	\$ 1,960.00
Tenable Technical Account Manager (TAM) Services			
TECH-SUP-PREM	Tenable Premium Support	\$ 40,000.00	\$ 39,200.00
TECH-SUP-ELITE	Tenable Elite Support	\$ 60,000.00	\$ 58,800.00
World Wide Technology Implementation & Managed Services			
PS-SUPP-1	World Wide Technology - Implementation & Managed Services for 1 Year - Per Device	\$ 25,000.00	\$ 6.47

**Tenable.io with Implementation, Training, and Managed Service
(Based on 100,000 Observable Objects)**

Initial Term Pricing (Years 1-3)

Item No.	Description	Rate Per User (A)
1	<u>Initial Software Year</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include: <ul style="list-style-type: none"> • Implementation • initial training • Initial Integration • integration maintenance • support services 	\$ 9.10
2	<u>Subsequent Software Year</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include: <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ 9.10

(Optional) Renewal Term Pricing (Years 4-6)

Item No.	Description	Rate Per User (A)
1	<u>Renewal Software Year (~15% increase from Year 1)</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include: <ul style="list-style-type: none"> • Implementation • initial training • Initial Integration • integration maintenance • support services 	\$ 10.47
2	<u>Subsequent Software Year (~5% YoY Increase)</u> One year of network-based asset discovery (agentless) software as described in the RFQ per user. To include: <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ 10.47

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
Tanium Waterfall Software SKUs			
TIOVM	Tenable.io Vulnerability Management Assets: 65 - 100,000 (Pricing Based on 100,000) - \$2.63 per object per year Term: 12 Months Tenable Public Sector LLC - TIOVM	\$ 314,090.00	\$ 263,484.20
TIOVM	Tenable.io Vulnerability Management Assets: 100,000+ (Pricing Based on 500,000) - \$2.40 per object per year Term: 12 Months Tenable Public Sector LLC - TIOVM	\$ 1,649,340.00	\$ 1,198,936.17
TIOVM-STNDC	Standard Tenable.io VM Container Term: 12 Months TENABLE.IO VM CONTAINER	\$ -	\$ -
World Wide Technology Implementation & Managed Services			
PS-SUPP-1	World Wide Technology - Implementation & Managed Services for 1 Year - Per Device	\$ 25,000.00	\$ 6.47

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
Tenable Waterfall Pricing			
TIOVM	Tenable.io Vulnerability Management Assets: 65 - 100,000 (Pricing Based on 100,000) - \$2.63 per object per year Term: 12 Months Tenable Public Sector LLC - TIOVM	\$ 314,090.00	\$ 263,484.20
TIOVM	Tenable.io Vulnerability Management Assets: 100,000+ (Pricing Based on 500,000) - \$2.40 per object per year Term: 12 Months Tenable Public Sector LLC - TIOVM	\$ 1,649,340.00	\$ 1,198,936.17

Item No. 3 – ACS Pricing Breakdown (Optional - But HIGHLY Recommended - Not included in Per Device Pricing)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
Optional Purchased Tenable Training			
TRG-TIO-ESS-SEAT	2 Day Seat - Access for 1 person to attend an available session of Tenable.io Essentials	\$ 2,000.00	\$ 1,960.00
Tenable Technical Account Manager (TAM) Services			
TECH-SUP-PREM	Tenable Premium Support	\$ 40,000.00	\$ 39,200.00
TECH-SUP-ELITE	Tenable Elite Support	\$ 60,000.00	\$ 58,800.00
World Wide Technology Implementation Services			
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Per Device	\$ 25,000.00	\$ 5.21



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:

ACS pricing is shown above in **Section III. Pricing.**

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.

Waterfall pricing is shown above in **Section III. Pricing.**

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.

No State of Florida Enterprise Pricing Provided

VII. Value-Added Services (Optional)

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

Please see section **"5) Detail regarding any value-added services"** on page 7 of this document.

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.

World Wide Technology, LLC

Vendor Name

43-1912895

FEIN

May 12, 2023

Date

Signature

Gregory Brush

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



4050 Esplanade Way
Tallahassee, FL 32399-0950

Ron DeSantis, Governor
Pedro Allende, Secretary

**CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT
BETWEEN
FLORIDA DEPARTMENT OF MANAGEMENT SERVICES
AND
WORLD WIDE TECHNOLOGY, LLC**

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

WHEREAS, Recipient has or will enter into a Purchase Order or Agency Term Contract under Request for Quote No. DMS-22/23-154, Network-Based Asset Discovery (Agentless) 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**

World Wide Technology, LLC

By: DocuSigned by:

5E91A9D369EB47C...

By: **Gregory Brush** Digitally signed by Gregory Brush
Date: 2023.05.12 14:01:26 -05'00'

Name: Pedro Allende

Name: Gregory Brush

Title: Secretary

Title: Area Vice President, Public Sector

Date: 6/14/2023 | 4:57 PM EDT

Date: May 12, 2023