FL [DIGITAL SERVICE]

Department of
MANAGEMENT
SERVICES

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

AGENCY TERM CONTRACT
FOR
Security Operations Platform
DMS-22/23-157H
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-22/23-157, Security Operations Platform; and

WHEREAS, the Department has accepted the Contractor's Quote and enters into this Contract in accordance with the terms and conditions of RFQ No. DMS-22/23-157.

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

1.0 Definitions

1.1 Agency Term Contract (ATC or Contract): A written agreement between the Department and the Contractor that is for use by the entire Department and under which Purchase Orders (PO) shall be issued.

1.2 Business Day: Any day of the week excluding weekends and holidays observed by State agencies pursuant to subsection 110.117(1)(a)-(j), Florida Statutes (F.S.).

1.3 Calendar Day: Any day in a month, including weekends and holidays.

1.4 Contract Administrator: The person designated pursuant to section 8.0 of this Contract.

1.5 Contract Manager: The person designated pursuant to section 8.0 of this Contract.

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

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

2.0 Scope of Work

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

3.0 Contract Term

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

4.0 Renewal Terms

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

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

5.0 Contract Documents and Hierarchy

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

1. Exhibit A: RFQ No. DMS-22/23-157.
2. Exhibit B: Contractor’s Quote.

In the event that any of the Contract documents conflict, the order of precedence set forth in Section 17.0, of RFQ No. DMS-22/23-157 shall control.

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

6.0 Amendments

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

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

7.0 Contract Notices

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

8.0 Contract Contacts

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

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

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

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 necessary Department, Purchaser, and Customer personnel, as required, to answer questions and resolve issues. The Contractor must provide written notice to the Department's Contract Manager if a new employee is designated as the Contractor's Representative for this Contract.

9.0 Assignment

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

10.0 Price Decreases

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

11.0 Additions/Deletions

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

12.0 Cooperative Purchasing

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

13.0 Other Conditions

13.1 Independent Contractor Status

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

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

13.2 Force Majeure

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

13.3 Cooperation with the Florida Senate and Florida House of Representatives

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

13.4 Employment of State Workers

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

SIGNATURE PAGE IMMEDIATELY FOLLOWS

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

ST. LOUIS BASED WORLD WIDE
TECHNOLOGY, INC.:

DocuSigned by:
E5C8AD825C76425...
Authorized Signature

Greg Brush
Print Name

AVP Public Sector
Title

6/30/2023 | 11:33 AM CDT
Date

STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES:

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

6/30/2023 | 12:37 PM EDT
Date

Exhibit "A"

Request for Quotes (RFQ)

DMS-22/23-157

Security Operations Platform Solution

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

1.0 DEFINITIONS

The following definitions shall apply throughout this RFQ:

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

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

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

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

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

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

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

Solution: An Extended Detection and Response (XDR) platform, which is a platform that combines multiple security technologies and tools, such as EDR (Endpoint Detection and

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

2.0 OBJECTIVE

Pursuant to section 287.056(2), F.S., the Department intends to purchase a security operations platform Solution for use by the Department and Customers to combine multiple security technologies and tools, such as EDR, NDR, and SIEM, into a single, integrated platform as specified in this RFQ.

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

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

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

3.0 DESCRIPTION OF PURCHASE

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

4.0 BACKGROUND INFORMATION

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

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

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

5.0 TERM

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

6.0 SCOPE OF WORK

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

6.1. Software Solution/Specifications

The Solution shall combine multiple security technologies and tools into a single integrated platform. The Solution must be designed to provide a comprehensive view of security posture, by consolidating security data from across the entire IT infrastructure. This enables security teams to quickly detect, investigate, and respond to security threats, with the goal of minimizing the impact of security incidents and reducing overall risk. In addition to integrating multiple security technologies, extended detection and response platforms typically leverage AI and machine learning to analyze large volumes of security data and automate threat detection and response processes. This can help reduce the burden on security teams and improve the speed and accuracy of security operations.

6.1.1. Multi-Tenant

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

6.1.2. Detection and Response

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

6.1.3. Scalability

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

6.1.4. Automation

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

6.1.5. Incident Reporting

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

6.1.6. User Management

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

6.1.7. Cloud Deployment

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

6.1.8. Threat Intelligence

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

6.1.9. Incident Response

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

6.1.10. Data Management and Storage

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

6.1.11. Performance Management

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

6.1.12. Disaster Recovery and Backup

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

6.1.13. Identity and Access Management

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

6.1.14. Network

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

6.1.15. Compliance and Third-Party Certification

The Solution shall comply with relevant standards like General Data Protection Regulation (GDPR), Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act, Personally Identifiable Information (PII) data requirements, Driver Privacy Protection Act, and third-party certifications such as Systems and Organizations Controls 2 (SOC 2) and International Organization for Standardization (ISO) 27001. The Department, Purchaser, or Customer may require Contractor(s) to execute security agreements, including but not limited to, CJIS riders or Business Associate Agreements as a condition of performance or purchase order issuance.

6.1.16. Integration

6.1.16.1. The Solution shall integrate with the Department's existing security tools such as firewalls, antivirus software, and SIEM systems. The Customer shall determine if the Solution is able to integrate with the Customer's security tools. The Contractor shall take any steps necessary to support Customer integration.

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

6.1.16.3. Initial Integration shall include connecting each Customer to the state Cybersecurity Operations Center (CSOC) and validating with FL[DS] that all Solution data is properly integrated, as requested by the Customer.

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

6.1.17. Performance and Availability

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

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

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

6.2. <u>Training and Support</u>

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

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

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

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

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

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

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

6.3. Kickoff Meeting

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

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

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

6.4. Implementation

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

The Implementation Plan must include the following at a minimum:

6.4.1. All tasks required to fully implement and complete Initial Integration of the Solution.

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

6.4.3. Dates that each task (or group of tasks) will be completed by, identify task dependencies, and tasks on the critical path to ensure timely project completion.

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

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

6.4.6. Provide Contractor contact information (name, title, email, and phone number) for the Contractor Representative who is assigned to oversee successful implementation and Initial Integration.

6.4.7. Document the frequency and method(s) for the Contractor to communicate the ongoing status of the Implementation Plan to the Purchaser and any other Customers.

6.5. Reporting

The Contractor shall provide the following reports to the Purchaser:

6.5.1. Quarterly Business Reviews (QBR) which will include, but not be limited to, performance reports and metrics on service level achievements. The Contractor shall schedule a quarterly meeting to review the QBR and document any financial consequences to be assessed as necessary.

6.5.2. Monthly Implementation Reports shall be provided to the Purchaser to document compliance with Final Implementation Plan(s) and document any financial consequences to be assessed as necessary.

6.5.3. Monthly Training Reports shall be provided to the Purchaser to document all training provided to the Purchaser and any other Customers and document any financial consequences to be assessed as necessary.

6.5.4. Monthly Service Reports shall be provided to the Purchaser to document Solution performance, availability, response times, and resolution times and document any financial consequences to be assessed as necessary.

6.5.5. Ad hoc reports as requested by the Purchaser.

6.6. Optional Services

6.6.1. Manage, Detect, and Respond (MDR)

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

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

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

6.6.2. Future Integrations

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

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

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

7.0 DELIVERABLES

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

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

TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES

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

TABLE 1 DELIVERABLES AND FINANCIAL CONSEQUENCES			
No.	**Deliverable**	**Time Frame**	**Financial Consequences**
3	The Contractor shall provide Solution access and all services in the Final Implementation Plan in accordance with this PO and any applicable ATC.	The Contractor shall provide Solution access and complete all requirements established in the Final Implementation Plan timely and accurately.	Financial consequences shall be assessed in the amount of $100 per calendar day, beginning on the first calendar day after any due date specified in the Final Implementation Plan, until the requirement is accurately completed. Financial consequences shall be assessed in the amount of $200 per requirement for each instance services are not performed, or documentation is not received, in accordance with this RFQ and the Implementation Plan.
4	The Contractor shall ensure the Solution is available in accordance with this PO and any applicable ATC.	The Solution must be available 99.999% of the time per month in accordance with the FL[DS]-approved SLA and. Compliance is calculated on a monthly basis for each Customer.	Financial Consequences shall be assessed against the Contractor in the amount of $100 for each negative deviation from the thousandth decimal point. For example, a Customer's monthly uptime of 99.997% will result in a financial consequence of $200, unless the Department accepts different financial consequence in the Contractor's Quote.
5	The Contractor shall ensure the Solution performs in accordance with the FL[DS]-approved SLA.	The Solution must perform in accordance with the FL[DS]-approved SLA.	Financial consequences shall be assessed in the amount of $100 per calendar day, beginning on the first calendar day after any due date specified in the FL[DS]-approved SLA, until the requirement is accurately completed, unless the Department accepts different financial consequence in the Contractor's Quote.

TABLE 1 DELIVERABLES AND FINANCIAL CONSEQUENCES			
No.	**Deliverable**	**Time Frame**	**Financial Consequences**
6	The Contractor shall ensure training and support are provided in accordance with the FL[DS]-approved SLA.	Training and support must be provided in accordance with Section 6.2. of this RFQ and the FL[DS]-approved SLA for training and support.	Financial consequences shall be assessed in the amount of $100 per calendar day, beginning on the first calendar day after any due date specified in the FL[DS]-approved SLA, until the requirement is accurately completed, unless the Department accepts different financial consequence in the Contractor's Quote.
7	The Contractor shall report accurate information in accordance with the PO and any applicable ATC.	QBRs are due 15 calendar days after the end of the quarter (January - March, April - June, July - September, and October - December). Monthly Implementation Reports are due five (5) calendar days after the end of the month. Monthly Training Reports are due five (5) calendar days after the end of the month. Monthly Service Reports are due five (5) calendar days after the end of the month. Ad hoc reports are due five (5) calendar days after the request by the Purchaser.	Financial consequences shall be assessed in the amount of $100 per calendar day, beginning on the first calendar day after any due date, until an accurate report is received.

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

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

8.0 PERFORMANCE MEASURES

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

8.1 Performance Compliance

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

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

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

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

9.0 FINANCIAL CONSEQUENCES

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

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

10.0 RESPONSE CONTENT AND FORMAT

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

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

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

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

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

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

11.0 TIMELINE

EVENT	DATE
Release of the RFQ	May 11, 2023
Pre-Quote Conference Registration Link: https://us02web.zoom.us/meeting/register/tZIlde6uqDkvG9QD2YQ4L4RJgTV_VFOdU23B	May 16, 2023, at 9:00 a.m., Eastern Time
Responses Due to the Procurement Officer, via email	May 22, 2023, by 5:00 p.m., Eastern Time
Solution Demonstrations and Quote Negotiations	May 23-25, 2023
Anticipated Award, via email	May 25, 2023

12.0 PROCUREMENT OFFICER

The Procurement Officer for this RFQ is:

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

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 <u>PUBLIC RECORDS AND DOCUMENT MANAGEMENT</u>

20.1 <u>Access to Public Records</u>

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 <u>Contractor as Agent</u>

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

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

RELATING TO THE PURCHASE ORDER, CONTACT THE FOLLOWING CONTACTS:

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

<u>OTHER PURCHASER</u>:
CONTRACT MANAGER SPECIFIED ON THE PO

20.3 Public Records Exemption

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

20.4 Document Management

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

21.0 IDENITIFICATION AND PROTECTION OF CONFIDENTIAL INFORMATION

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

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

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

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

22.0 USE OF SUBCONTRACTORS

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

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

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

23.0 LEGISLATIVE APPROPRIATION

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

24.0 MODIFICATIONS

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

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

25.0 CONFLICT OF INTEREST

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

26.0 DISCRIMINATIORY, CONVICTED AND ANTITRUST VENDORS LISTS

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

27.0 E-VERIFY

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

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

28.0 COOPERATION WITH INSPECTOR GENERAL

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

29.0 ACCESSIBILITY

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

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

30.0 PRODUCTION AND INSPECTION

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

31.0 SCRUTINIZED COMPANIES

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

32.0 BACKGROUND SCREENING

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

32.1 Background Check

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

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

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

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

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

32.2 <u>Disqualifying Offenses</u>

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 <u>Refresh Screening</u>

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 <u>Self-Disclosure</u>

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

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

32.5 Duty to Provide Security Data

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

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

32.6 Screening Compliance Audits and Security Inspections

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

32.7 Record Retention

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

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

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

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

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

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

32.8 Indemnification

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

33.0 LOCATION OF DATA

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

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

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

34.0 DATA TRANSMISSION

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

35.0 TERMS AND CONDITIONS

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

36.0 COOPERATIVE PURCHASING

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

37.0 PRICE ADJUSTMENTS

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

38.0 FINANCIAL STABILITY

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

39.0 RFQ ATTACHMENTS

Attachment A, Price Sheet
Attachment B, Contact Information Sheet
Agency Term Contract (Redlines or modifications to the ATC are not permitted.)
Department's Purchase Order Terms and Conditions
Non-Disclosure Agreement (Redlines or modifications to the NDA are not permitted.)

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT A
PRICE SHEET

I. Alternate Contract Source (ACS)

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

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

______ 43230000-NASPO-16-ACS Cloud Solutions

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

II. Pricing Instructions

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

III. Pricing

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

Optional Renewal Term Pricing (Years 4-6)		
Item No.	**Description**	**Rate Per User**
1	**<u>Initial Software Year</u>** One year of security operations platform software Solution as described in the RFQ per user. To include: • **implementation** • **initial training** • **initial Integration** • integration maintenance • support services	$ ___________
2	**<u>Subsequent Software Year</u>** One year of security operations platform software Solution as described in the RFQ per user. To include: • **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 a security operations platform at no additional cost to the Department, the vendor may offer the Department value-added services, in addition to the services and/or commodities expressly sought by this RFQ.

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

______________________________ ______________________________
Vendor Name Signature

______________________________ ______________________________
FEIN Signatory Printed Name

____
Date

The State of Florida

Department of Management Services

Security Operations Platform Solution

RFQ Number DMS-22/23-157

Cloud Solutions (43230000-NASPO-16-ACS)

May 22, 2023

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

wwt.com

May 22, 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 Security Operations Platform Solution**

Dear Ms. Morgan:

Thank you for inviting World Wide Technology (WWT) to present the State of Florida, Department of Managed Services (the Department) with a Security Operations Platform (SOP) Solution that combines multiple security technologies and tools into a single integrated platform with enterprise-wide visibility to guard against a wide range of security threats. Our solution showcases how our integration capabilities easily coalesce the goals of recently released RFQs, including DMS-22/23-157, and make the Department's Enterprise Cybersecurity Resiliency Program a world-class model for the nation.

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

For this project, WWT supplies a multi-tenant security platform that allows organizations statewide to independently operate within the same system while having separate data storage and access controls. This AI and machine learning enhanced platform aggregates all the tenants' instances to provide comprehensive visibility and automated processes to quickly detect, investigate and respond to security threats. Our solution incorporates incident reporting, user management and scalability, delivering on all Section 6.0 requirements including, cloud, data, storage, performance, identity and access management tools and methods. Also, our proposal creates a consortium contract with access to waterfall pricing for city, county and state agency security needs, empowering lower revenue-generating cities and counties to affordably acquire software, implementation, training, support and integration services WWT offers.

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 Statues, Rule Title 60GG, Florida Administrative Code (F.A.C.) and other cybersecurity best practices.

Our staff's experience with sensitive security projects and their behavioral analysis, machine learning and threat intelligence based approach optimizes the Department's security posture

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 Endpoint Detection and Response Solution 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, Tenable, Elastic and Fortinet for this RFQ. Our collaborative approach involves a comprehensive reach across 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 its security architecture.

WWT sandbox environments allow our security strategy to adjust as threats evolve

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 our partners' security solutions to provide robust containment, isolation and remediation guidance against malicious activity. These labs also facilitate many more optimization methodologies to drive testing and secure outcomes.

WWT's past accomplishments with security projects assure the success of DMS-22/23-157

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, pull in resources to scale, 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:

- Optimized threat response for a customer SOC by automating phishing email manual tasks for the SOC to reduce response times
- Integrated multiple threat feeds to a Security Operations Platform to increase visibility, prioritize threat remediation and mitigate risk
- Designed security architectures for customers to integrate and automate security solutions to reduce the cyber kill chain timeframe and reduce risk

WWT believes in the power of uniting employees, customers, partners and communities against cyber threats. We have a successful track record working with the State of Florida, technology vendors, customers and other integrators to increase security maturity and capabilities. As adversaries become more cunning, skilled and innovative, WWT wants to collaborate on the Department's Security Operations project to continue improving security processes and policies from Tallahassee to Key West.

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

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

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

Tanium is a comprehensive security operations platform that offers organizations a wide array of capabilities to strengthen their security infrastructure. With its holistic approach, Tanium enables security teams to efficiently monitor, manage, and respond to security threats across their IT environment. Its real-time monitoring and data aggregation capabilities provide deep visibility into endpoints, servers, and network infrastructure, empowering security professionals to proactively identify vulnerabilities and swiftly respond to potential threats. Additionally, Tanium's advanced threat detection and response capabilities, coupled with its integrated approach to incident management, streamline the entire process of threat hunting and incident response, allowing organizations to rapidly mitigate risks and minimize the impact of security incidents.

Another crucial aspect of Tanium's comprehensive offering is its robust endpoint management features. By providing centralized control and automation, organizations can efficiently manage software distribution, patch management, configuration settings, and asset inventory. This ensures that endpoints remain secure and up-to-date, reducing the attack surface and strengthening overall security posture. Tanium's endpoint management capabilities offer organizations the ability to enforce security policies, remediate vulnerabilities, and maintain compliance, all within a unified platform.

In summary, Tanium stands as a powerful security operations platform that empowers organizations to enhance their security defenses. Its comprehensive range of capabilities, including real-time visibility, advanced threat detection, incident response, and endpoint management, equips security teams with the tools they need to proactively protect their systems, swiftly respond to incidents, and maintain a secure IT environment.

The Core Platform provides powerful capabilities for interacting and reporting on devices, regardless of device type or location, with a variety of features including Interact, Trends, Connect and Impact. Interact- A natural language parser allowing questions to be structured in plain English and enabling users of all skill levels.

- **Trends** - enables continuous measurement and reporting on key metrics such as hardware and software inventory.
- **Connect** - An integration layer that enriches external or 3rd party systems with up to the second data from every endpoint in the environment. Connect can feed endpoint data into SIEMS, log analytics tools, CMDBs and more.

In addition to the Core Platform, Tanium's Asset, Discover, Patch, Deploy, Performance, Threat Response Provision, and Enforce modules will satisfy the requirements of this request. Here is a detailed overview of the included modules:

Tanium Asset

Get a comprehensive inventory of hardware and software assets across the enterprise. With Tanium Asset, DMS will get real-time data about IT assets, regardless of location. These rich insights will help Florida make the right decisions about managing their devices and systems efficiently.

Automate Asset Reporting With Speed and Accuracy Quickly and easily find, inventory and maintain IT assets. Tanium's approach to endpoint visibility and control allows IT teams to take a real-time inventory of hardware and software assets. Utilize automated and predefined reports and dashboards with details by department, location, user group, and more.

Configurable Reporting for Inventory and Audit Preparation Make data-informed decisions about hardware and software across the environment. Extract insight for all assets within seconds and run quick configurable reports to help streamline inventory and audit preparation. Make the right changes around software licensing depending on usage, or on hardware decommissioning based on asset location—remote, on premises, or in the cloud.

Third-Party Data Enrichment Increase throughput by reclaiming underutilized assets and improve reporting from third-party data stores. Organizations depend on the accuracy of Configuration Management Database (CMDB) information. Tanium Asset feeds real-time data into common CMDBs, such as ServiceNow, so you have the freshest and most accurate information. For offline devices, Tanium Asset provides reporting on the last known state of the device.

Tanium Discover
Find and take control of unmanaged endpoints across remote, on-premises and cloud environments. Security hygiene begins with knowing what's connected to your network. Tanium Discover scans networks with hundreds of thousands of endpoints to find unmanaged assets. Administrators can choose to block the devices or bring them under management.

Quickly and Easily Find Unmanaged Assets on Complex Networks Gain comprehensive visibility and control of managed and unmanaged endpoints, regardless of location. Tanium Discover detects hidden, unmanaged assets across large, distributed networks. Unlike approaches that depend on wide-area network (WAN) links, which take hours or weeks to complete, the Tanium platform actively monitors and scans local subnets for unmanaged assets and reports on newly discovered and lost assets that were previously managed.

Collect and Analyze Detailed Endpoint Data Use detailed information about your devices to make informed management decisions. For every device it finds, Tanium Discover shows the hostname, MAC and IP addresses, device manufacturer, OS, open ports/ applications, and historical information such as the first and last time the unmanaged asset was seen on the network. Administrators can choose from multiple scanning options for different environments.

Secure and Take Control of Unmanaged Assets Discover unmanaged assets and quickly bring them into a managed and secure state. Once unmanaged devices are found, administrators can deploy the Tanium agent on rogue endpoints to bring them under management or block them from the network. These events can be exported to a SIEM or incident management system for further analysis.

Tanium Patch
Simplify and accelerate patch management and compliance. With Tanium Patch, IT teams can keep systems up to date with automated patching across the enterprise, at speed and scale. This helps organizations reduce complexity and increase business resilience.

- Mitigate risk, maintain compliance and reduce disruption: To prevent security breaches, keep endpoints up to date with the latest patches.

- Reduce overhead and complexity: Patch at scale with little to no infrastructure and minimal downtime.
- Patch With confidence: Measure cyber hygiene with real-time patch success rates across the organization.
- Real-time patch visibility and control: Tanium designed our platform architecture to maintain performance across hundreds of thousands of endpoints. The Tanium platform provides speed and scale to help ensure endpoint patches happen quickly without fail.
- One client, no extra agents or infrastructure: Patch hundreds of thousands of systems on a single Tanium instance, without the need for secondary relay, database or distribution servers at different bank branches, retail locations, or geographically dispersed offices.
- Customized patch scheduling and workflows: Deploy a single patch to a computer group immediately or perform more complex tasks. For example, use advanced rule sets and maintenance windows to deliver groups of patches across your environment at specified times.
- Patching effectiveness tracking: Tanium Patch summarizes the deployment status for any patch, providing immediate feedback on successes as well as failures requiring remediation. It also gives patch histories for individual machines, endpoint reboot status and links to relevant vendor knowledge base articles.

Tanium Deploy

Quickly install, update or remove software across your environment. With Tanium Deploy, IT operations teams can simplify software installation, maintenance, and removal. This helps organizations run far more effectively while reducing complexity and improving business resilience.

- Manage software efficiently: Reduce your time spent deploying updates and fixes. Reduce overhead and complexity: Update at scale with little to no infrastructure and without fear of downtime. Streamline IT ops and empower end users: Let users manage their software on their schedule through a self-service portal.
- -Software package management workbench: Tanium Deploy dramatically accelerates system deployment and updating. The Tanium Deploy package management workbench simplifies software management functions by reducing the time it takes to build, maintain and distribute software packages.
- Third-party software updates: Tanium Deploy includes templates for importing and deploying third-party software. Operations teams no longer need to browse websites for the latest updates or create deployment packages. Instead, they can identify and resolve new vulnerabilities.
- One client, no extra agents or infrastructure: The Tanium platform offers speed and scale to help ensure software changes happen quickly on endpoints without fail. The Tanium architecture maintains performance across hundreds of thousands of endpoints on a single Tanium server.
- End-user self-service portal: Tanium Deploy allows IT Administrators to let users install, update and remove approved and assigned software through easy-to-setup Self-Service Profiles and Self-Service Client Applications.

Tanium Enforce

Unified policy and configuration management at scale. Tanium Enforce allows organizations to simplify, centralize and unify policy and configuration management of end user computing devices.

Enhanced policy management for Windows: Tanium Enforce can manage policies for Windows on and off domain, on premises or in remote locations all from a single console. Centrally manage Windows policies for client and server operating systems throughout your organization, at scale.
Modern Device Management for macOS: Modern Device Management for macOS (MDM) provides policy configuration and patch management, Mac endpoint provisioning and remote wipe all from the Tanium console for macOS 11.x or higher.

USB removable storage management: Tanium Enforce with USB removable storage management can protect your endpoints from unauthorized USB devices, malware introduction and data exfiltration.
Firewall management: Effective endpoint firewall management requires dynamic, micro-segmentation of an organization's endpoints. Help ensure only approved processes and applications communicate on trusted ports.

Antivirus management: With Tanium Enforce, leverage native AV capabilities by completely managing and configuring Defender across the organization.

Endpoint encryption: Encrypting data at rest is essential if endpoints were lost, stolen or inappropriately decommissioned. Tanium Enforce can manage native OS drive encryption offered by Apple FileVault and Microsoft BitLocker.

Tanium Threat Response

Eases the collaboration challenges faced by security and IT teams, providing an integrated view across your digital infrastructure.

- Enhance security and mitigate risk: Minimize the impact of threats with automated hunting, early detection, and rapid investigation and remediation.
- Detect suspicious behavior in seconds at scale: Identify compromised endpoints and stop suspicious behavior in seconds.
- Minimize business disruption: Minimize impacts to your business and isolate advanced malware in real time.
- Real-time endpoint monitoring: Tanium Threat Response continuously monitors endpoints for suspicious activity whether they're online or offline. Real-time alerting with Tanium Signals gives security teams immediate notice when anomalies occur so they can investigate. Users can also create custom signals for tailored detection.
- Forensic investigations: Remotely conduct forensic investigations on suspicious machines. Employ enterprise-wide searches of each endpoint. Quarantine compromised machines or take targeted actions, such as halting malicious processes, capturing files, alerting users and closing unauthorized connections and much more.
- Incident response and remediation: Tanium Threat Response adapts to incidents, so organizations can fully understand them by using remote forensic investigation on suspicious machines. Take a wide variety of remedial actions, such as imposing network quarantines, deploying patches or running custom scripts.

Tanium Performance

Monitor, investigate and remediate end-user performance issues quickly and at scale. Tanium Performance allows organizations to track critical performance metrics related to hardware resource consumption, application health and system help. Gain insights from rich historical data and boost the efficiency of your IT team.

Improve IT Efficiency Monitor and be notified on critical performance metrics. Monitor metrics related to hardware resource consumption, application health and system health, such as CPU utilization, disk latency and application crashes. Specify negative performance event thresholds and send notifications to the IT Team.

Quickly troubleshoot with context. Investigate endpoint performance problems using live and historical process-level resource consumption data. To better identify root causes, access important attributes about the endpoint such as CPU model and memory capacity.

Improve End-User Experience Analyze and evaluate the end-user experience. Analyze end-user performance data across an environment. Understand commonalities between trends, such as top resource-consuming processes by computer models. Dive deeper into results by filtering endpoint data by computer group and time period.

Resolve issues non-invasively. In a modern distributed workforce, find and fix problems without requiring end-user interaction. Review historical and current performance data as well as browse the endpoint file system, all from the Tanium console, without disrupting the end-user's workday. The result: increased employee productivity.

Tanium Comply
Identify vulnerability and compliance exposures within minutes across widely distributed infrastructures. Tanium Comply conducts vulnerability and compliance assessments against operating systems, applications, and security configurations and policies. It provides the data necessary to help eliminate security exposures, improve overall IT hygiene and simplify preparation for audits.

- Support for industry-specific, security best practices or custom checks
- Tanium Comply supports the Security Content Automation Protocol (SCAP) and can employ any Open Vulnerability and Assessment Language (OVAL)-based content, including custom checks. The Tanium content library updates daily with the most current vulnerability and compliance data.
- Exposure drill-down and fix Seamlessly transition from identifying a vulnerability within Tanium Comply to launching remediation activities such as patching, software updates or policy and configuration changes from the Tanium platform.
- Alignment with regulatory and corporate requirements Organizations can use Tanium Comply to help fulfill configuration hardening and vulnerability scanning portions of industry regulatory requirements, including PCI, HIPAA and SOX. The freedom to conduct ad hoc scans also improves adherence to corporate mandates for proactive security assessments.

Tanium Reveal
Locate and manage sensitive data across endpoints to mitigate exposure.
Delivering results in real time, Tanium allows you to quickly search for sensitive data across endpoints at scale, helping improve efficiencies through risk inventory and compliance audit cycles.

- **File formats and operating systems tracking** Locate, categorize and manage personally identifiable information, personal health information and sensitive project keywords in a wide variety of common file formats on Windows, Mac and Linux endpoints. Take action on demand to address issues.

- **Tanium index tool** Indexes local file systems and key attributes, recording the information in an SQLite database directly on the endpoint. This improves detection and reporting on files at rest on the device using minimal resources.
- **Out-of-the-box regulatory content** Use default content to enhance visibility into GDPR, PCI, HIPAA and CCPA use cases. Detect personal information, financial information and free-form text strings in previously unmanaged files.

Tanium SBOM
Know all your software supply chain vulnerabilities in seconds.
We won't know what the next supply chain vulnerability is going to be, but with Tanium, know how your applications are affected before it happens so that when it does, you're ready to take action.

- **Know every software package** Identify all runtime libraries, open-source freeware and software packages at the click of a button.
- **Enable granular decision-making** Make nuanced decisions about your applications based on your organization's risk tolerance.
- **Take action based on your needs** Remediate the SBOM item in the manner that best suits your organization, using the flexibility of Tanium.

Tanium Benchmark
Compare and prescriptively improve your IT risk metrics against your industry peers.

- **Better collaboration** Report risk scores and benchmarks to improve understanding and insight.
- **Understand your IT risk** Get real-time information on all your endpoints and identify vulnerability and compliance gaps.
- **Reduce attack surfaces** Improve your cyber hygiene to minimize endpoint cyber risk.

Tanium Certificate Manager
Real-time visibility into your digital certificates
Don't let an unknown or expired certificate ruin your day. Modernize your certificate management and enable your organization to have real-time visibility and control of certificates.

- **Discover what certificates you have in your environment** Mitigate your risk of business outages because you can't manage what you can't see.
- **Identify where your certificates are from** Don't fall victim to rogue certificates from unauthorized Certificate Authorities.
- **Know which certificates are vulnerable and expiring** Proactively know when you need to renew your certificates.
- **Tanium Integrity Monitor** Efficiently monitor file and registry changes, simplify compliance at scale. Tanium Integrity Monitor employs speed, visibility and control to deliver comprehensive registry and file integrity monitoring at scale.
- **Tanium client recorder** The Client Recorder Extension monitors the endpoint kernel and other low-level subsystems to capture a variety of events. As events occur, the Tanium Recorder captures a comprehensive, easy-to-interpret history of the who, what, when, where and how.
- **Multi-operating systems support** Tanium Integrity Monitor supports Windows, Linux, Solaris and AIX operating systems, incorporating them into an integrated workflow and reporting structure.

- **Dynamic data review and classification** Investigate recent events and perform follow-up or drill-down actions with ease. Automatically label or categorize events using rules, defined criteria or event information in order to improve the signal-to-noise ratio and reduce false positives.
- **Watchlist templates aligned to standards** Create your own configuration or utilize pre-built templates to address regulatory frameworks including PCI-DSS, CIS Critical Security Control 3, HIPAA, SOX and NERC-CIP. Integrity Monitor includes watchlist templates with critical files, directories and registry items for Windows and Linux systems.

Tanium Impact
Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Tanium Provision
Tanium Provision reduces the need for dedicated hardware by enabling any Tanium Client to act as a PXE Service for that network segment. Provision provides bare-metal provisioning of Microsoft Windows or Linux to on-premises and internet-connected devices. It also enables re-imaging outdated or broken devices.

- Bare metal provisioning of Windows and Linux using distributed PXE and USB devices
- Ongoing software updates, patching and operating system upgrades
- Creation of OS Bundles
- An *OS bundle* includes all the files and settings that an operating system deployment requires. You can create an OS bundle for each Windows or Linux version, or for unique configurations that you can use for location, hardware, or business processes.
- Creation of OS Refreshes
- An *OS refresh deployment* is used to refresh an existing system with a selected OS bundle.
- Utilize PXE Endpoints
- A *Preboot eXecution Environment (PXE) endpoint* is an endpoint that runs a service to provide required content for clients. The TaniumPXE service provides the PXE endpoint capabilities. You can boot devices from a PXE network or from USB media.
- Utilize Offline Domain Join

If you want newly-deployed Windows endpoints to join an Active Directory (AD) domain, you can use Tanium Provision to set up an offline domain join (ODJ) process. Provision uses ODJ functionality to join newly-deployed Windows endpoints to AD.

Interoperability with Other Tanium Products Provision works with Tanium™ Direct Connect to provide additional features.

Direct Connect
You can use Provision to deploy the Tanium PXE service on Windows, Windows Server, macOS, or Linux satellites and optionally use Windows satellites to set up ODJ for provisioning endpoints. Provision also includes a direct link to create satellites in Direct Connect from the **Create Provision Endpoint** process.

Training
Tanium training provides enhanced knowledge and understanding of Tanium products giving users the confidence they need to expand their abilities and get the most out of their Tanium deployment.

- Web Based Training Tanium's web-based training offers numerous benefits, including the flexibility to learn at one's own pace and convenience, eliminating the need for travel or fixed training schedules. It provides interactive and engaging content, allowing participants to acquire comprehensive knowledge about Tanium's solutions and effectively utilize them to enhance security, streamline operations, and optimize IT management practices.
- Instructor Lead Training Tanium's instructor lead training allows for direct interaction with experienced trainers, facilitating real-time Q&A sessions, personalized guidance, labs, and the opportunity to learn from their practical experience. Additionally, hands-on labs and demonstrations can be effectively conducted, enabling participants to gain practical skills and confidence in utilizing Tanium's solutions.
- Certifications & Exams - Maximize the potential of Tanium features and functionality in your environment by validating technical capabilities with Tanium career certifications. By ensuring professionals are skilled and knowledgeable about Tanium, an organization can accelerate business value and truly utilize the power of Tanium.

Support: Technical Account Management & Support Center

- Technical Account Management: Tanium's Technical Account Management (TAM) model is designed to provide customers with personalized support and guidance throughout their journey with Tanium. TAMs are experienced technical experts who work closely with customers to understand their unique requirements, challenges, and goals. They serve as trusted advisors, offering strategic recommendations, best practices, and tailored solutions to help customers maximize the value of their Tanium deployments.

  TAMs collaborate closely with customers to develop a deep understanding of their IT environment, workflows, and business objectives. They assist in the planning, implementation, and optimization of Tanium solutions, ensuring alignment with customer-specific needs. TAMs also provide proactive monitoring, performance assessments, and regular health checks to identify potential issues and optimize system performance.

  Furthermore, TAMs act as one of the primary points of contact for customers, facilitating effective communication and coordination with Tanium's support, product, and engineering teams. They provide ongoing training, workshops, and knowledge transfer sessions to ensure customers have the necessary skills and understanding to leverage Tanium effectively.

  Through the TAM model, Tanium aims to foster long-term partnerships with customers, delivering continuous value, and driving successful outcomes. By combining technical expertise, strategic guidance, and personalized support, the TAM model helps customers optimize their IT operations, enhance security, and achieve their business objectives using Tanium's solutions.
  - Support Center: Tanium's Support Center serves as a comprehensive resource hub for customers, providing them with the necessary assistance and guidance to maximize the value of their Tanium solutions. The Support Center offers a range of self-service tools, including a knowledge base, documentation, and community forums, enabling users to find answers to their queries and access relevant information easily. Additionally, customers can directly engage with Tanium's support team through various channels, such as phone, email, or the online support portal, ensuring timely resolution of issues and efficient troubleshooting. With its focus on customer success, Tanium's Support Center plays a vital

role in ensuring smooth implementation, continuous operation, and ongoing support for Tanium users.

- Tanium Enterprise Services: Tanium's services organization plays a vital role in delivering exceptional value to customers. Comprised of a team of experienced professionals, the services organization works closely with clients to ensure successful implementation, optimization, and ongoing support of Tanium solutions. They provide a wide range of services, including consulting, project management, technical training, and support. With their deep expertise and customer-centric approach, Tanium's services organization helps organizations maximize the benefits of Tanium's solutions, streamline IT operations, enhance security, and achieve their business objectives.

6.1. Software Solution/Specifications

6.1.1. Multi-Tenant

The Solution shall support a multi-tenant architecture, allowing multiple organizations or departments to securely and independently operate within the same system, with separate data storage and access controls.

Tanium provides both single tenant and multi-tenant, multi-organization architectures. This flexibility enables organizations to have options while still being able to aggregate data and information up to a single view for enterprise security operations via the Tanium Connect module. This allows for easy management of multiple organizations, while also providing single-source visibility into threats, investigations, and trends. Additionally, Tanium provides customizable dashboards that can be tailored to meet the needs of each organization or individual further enhancing the multi-tenant capabilities of the solution. Customers who fall below a certain threshold in terms of size may find it more economical to opt for a multi-tenant architecture rather than a single tenant architecture. Additionally through using Role Based Access Control (RBAC), Tanium allows a single tenant to be used while adding multiple organizations within the single tenant.

6.1.2. Detection and Response

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

Tanium detects and responds to various security threats, including malware, phishing, insider threats, and zero-day attacks.

6.1.3. Scalability

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

Tanium offers exceptional scalability, making it an ideal solution for organizations of all sizes. The platform can easily scale to support a large number of tenants and their endpoints, ensuring that the solution can grow alongside the business. In fact, Tanium has several customers with over a million endpoints, highlighting its ability to support large and complex IT environments. With its scalable architecture, Tanium provides organizations with a flexible and adaptable endpoint management solution that can meet their changing needs over time. Additionally, through using Role Based Access

Control (RBAC), Tanium allows a single tenant to be used while adding multiple organizations within the single tenant.

6.1.4. Automation

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

Tanium empowers organizations with the ability to automate responses to security threats, streamlining incident response and reducing manual intervention. Leveraging its powerful automation capabilities, Tanium can swiftly initiate predefined actions to contain and mitigate threats as soon as they are detected.

When a security threat is identified, Tanium can automated to trigger response actions such as isolating affected endpoints from the network, restricting access privileges, or initiating remediation steps. This automated response helps prevent the lateral movement of threats and minimizes their impact on the environment.

6.1.5. Incident Reporting

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

Tanium offers detailed reporting on security incidents, including alerts, investigations, and remediation activities.

Tanium provides robust reporting capabilities, enabling organizations to gain visibility into endpoint hardware and software inventory, configuration, and compliance anomalies, device status, owners, and locations. With out-of-the-box reports, organizations can quickly access critical information, while customizable reports allow them to tailor reporting to their specific needs. Automated reporting further streamlines the process, providing regular, scheduled reports without the need for manual intervention. Tanium's reporting capabilities allow organizations to make data-driven decisions, identifying trends, and potential issues before they become problems. With Tanium's reporting, organizations can optimize their IT operations, improve compliance, and enhance security.

6.1.6. User Management

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

Tanium offers a comprehensive Role-Based Access Control (RBAC) feature to enable organizations to define and enforce access control policies based on the principle of least privilege. RBAC is designed to help organizations reduce the risk of unauthorized access, data breaches, and insider threats by providing granular control over what users can do within the system. The Tanium RBAC feature allows organizations to create customizable role-based personas based on responsibility, which can be assigned to individual users or groups of users. These personas determine the level of access to Tanium functionality and data that users have. For example, an organization might create roles such as "Endpoint Technician," "Security Analyst," or "System Administrator," each with its own set of permissions and restrictions. Tanium RBAC also allows organizations to define roles and permissions based on specific business units or departments, ensuring that users only have access to the data and functionality they need to perform their job responsibilities. Additionally, Tanium RBAC includes the ability to create custom roles and to modify existing roles to meet changing business needs. In terms of enforcement, Tanium RBAC includes built-in audit and reporting capabilities, which provide visibility into who is accessing what data and functionality within the system. This helps organizations identify potential security risks and track down suspicious activity. Overall, Tanium RBAC is a powerful tool for managing access to Tanium functionality and data and for reducing the risk of unauthorized access and data breaches.

6.1.7. Cloud Deployment

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

Tanium is highly deployable in cloud environments, supporting multi-cloud deployments. It can seamlessly integrate with various cloud platforms, allowing organizations to leverage the benefits of cloud computing while utilizing Tanium's powerful capabilities for endpoint management and security. With its flexible architecture, Tanium can adapt to different cloud infrastructures, enabling efficient and scalable deployments across multiple cloud providers.

6.1.8. Threat Intelligence

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

Tanium leverages threat intelligence for enhanced threat detection and response. By integrating with various threat intelligence sources, Tanium can provide valuable contextual information about threats, including indicators of compromise (IOCs), known malicious IP addresses, and suspicious file hashes. This enables organizations to quickly identify and prioritize potential security incidents, leading to faster and more accurate response actions.

6.1.9. Incident Response

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

Tanium supports incident response workflows by integrating with playbooks and case management systems, enhancing response efficiency and effectiveness.

6.1.10. Data Management and Storage

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

Tanium provides robust data management capabilities to ensure data privacy, security, and compliance. Tanium Cloud protects data used within Tanium and offers encryption and security for data at rest and in motion, allowing organizations to monitor, report, and manage data sharing. Tanium also provides data visibility and control by tracking data usage, movement, and access. This helps organizations to manage their data more effectively, ensuring that sensitive information is kept secure and only accessed by authorized personnel. Overall, Tanium's data management capabilities help organizations to better protect their sensitive data and comply with data privacy regulations.

6.1.11. Performance Management

The Solution shall provide proactive alerts on system events, as well as logging and resolution

reporting on all issues.

Tanium provides proactive alerts on system events and logging to help identify and resolve issues. The Tanium Connect module can also send alerts and other data to external systems like a SIEM or ticketing system, as well as data lakes for advanced analysis and correlation. This allows for a more streamlined approach to incident response and provides greater visibility into potential security threats. With Tanium Connect, security teams can quickly identify and respond to security incidents, improving their overall security posture. Tanium offers a Performance module that provides real-time monitoring and analysis of endpoint performance, including resource utilization, process activity, network usage, and more. The module helps identify potential issues and bottlenecks, allowing IT teams to proactively address them before they impact endpoint performance. The data collected by the Performance module can be sent to external systems using the Tanium Connect module, which allows for integration with SIEMs, ticketing systems, or data lakes. This enables IT teams to aggregate and correlate endpoint performance data with other system events for more comprehensive insights into the overall health of their environment.

6.1.12. Disaster Recovery and Backup

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

Tanium offers a comprehensive data management and storage solution that meets the requirements for data storage capacity, file types, and locations. The Tanium Cloud provides a secure and scalable infrastructure to store and manage data collected from endpoints. The solution includes disaster recovery processes to ensure business continuity in case of unexpected events, and rollbacks in case of errors or issues. Tanium also provides extraction and eradication processes to ensure compliance with data protection regulations and guidelines. With Tanium's data management and storage capabilities, organizations can ensure the security and integrity of their data, meet regulatory compliance requirements, and access data in a timely and efficient manner.

6.1.13. Identity and Access Management

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

Tanium offers seamless integration with popular Identity and Access Management (IAM) tools such as Azure AD, Okta, Cyberark, and Ping Identity, to name a few. This integration provides users with a unified authentication and authorization mechanism that enables a seamless and secure access experience to Tanium's endpoint management and security solutions. With the integration, Tanium leverages the capabilities of these IAM tools, including user authentication, password policy management, two-factor authentication, single sign-on, and role-based access control, to ensure that the right users have access to the right data at the right time, and that all activities are properly audited and monitored.

6.1.14. Network

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

Tanium integrates with network technologies to provide optimal performance of the solution. Tanium has a unique and patented network communications architecture to ensure efficient and effective network communication between endpoints and the Tanium Cloud. Additionally, Tanium's linear chain architecture helps to minimize network traffic and improve performance. The Tanium Performance module also provides insights and tracking for network traffic and performance, helping to identify and resolve issues quickly. By leveraging these network technologies and tools, Tanium provides a reliable and efficient endpoint management solution.

6.1.15. Compliance and Third-Party Certification

The Solution shall comply with relevant standards like General Data Protection Regulation (GDPR), Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act, Personally Identifiable Information (PII) data requirements, Driver Privacy Protection Act, and third-party certifications such as Systems and Organizations Controls 2 (SOC 2) and International Organization for Standardization (ISO) 27001. The Department, Purchaser, or Customer may require Contractor(s) to execute security agreements, including but not limited to, CJIS riders or Business Associate Agreements as a condition of performance or purchase order issuance.

Tanium takes compliance and security seriously, ensuring that its solution meets relevant industry standards and third-party certifications. Tanium is compliant with various regulations like certifications like ISO 27001. Tanium also allows for the execution of mutually agreeable security agreements, including CJIS riders or Business Associate Agreements, as required by the Department, Purchaser, or Customer. By adhering to these standards and certifications, Tanium provides a secure and trustworthy endpoint management solution that can be trusted to protect sensitive data and meet compliance requirements. Supplier and third-party security and privacy requirements are established through vendor security and diligence reviews, in coordination between procurement, legal and GRC. Contracts are maintained in accordance with the services to be provided and legal/local/regulatory/compliance requirements. The standard contract reviews for third party suppliers cover IT and cybersecurity provisions, controls and requirements, as well as consideration for legal and regulatory requirements, incident reporting, SLAs, RTOs, service continuity and service termination. Tanium's Data Processing Agreement (DPA) outlines the company's commitment to compliance with the European Union's General Data Protection Regulation (GDPR) and other data protection laws. The DPA provides customers with a detailed explanation of how Tanium collects, processes, and protects personal data, as well as their rights as data subjects. Tanium's DPA also includes the necessary clauses and guarantees to ensure that customers can comply with their own GDPR obligations when using Tanium's endpoint management solution. See more info at www.tanium.com/dpa Additional information provided upon request.

6.1.16. Integration

6.1.16.1. The Solution shall integrate with the Department's existing security tools such as firewalls, antivirus software, and SIEM systems. The Customer shall determine if the Solution is able to integrate with the Customer's security tools. The Contractor shall take any steps necessary to support Customer integration.

Tanium is designed to integrate with a wide range of security tools, including firewalls, antivirus software, endpoint management solutions, and SIEM systems. Tanium can work with the Department's existing security infrastructure. The Customer has the flexibility to determine if the Customer's security tools are able to integrate with the Solution, and if so, at what level, with the Customer's security tools and the Contractor(s) can assist in this determination as necessary. The Contractor(s) will take all necessary steps to support the integration should the Customer decide to move forward. Tanium's robust integration capabilities make it easy to integrate with existing security infrastructure, enabling effective management and protection of endpoints.

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

Tanium Cloud can be integrated with various identity and access platforms such as OneLogin, Auth0, Duo Access Gateway, Azure AD, Okta, AD FS, Oracle Identity Cloud Service, PingFederate, Google Cloud Identity, Salesforce and others. By configuring these platforms, users can easily access Tanium Cloud while ensuring secure authentication and authorization processes. This integration enables organizations to efficiently manage user access to the Tanium Cloud platform, improve security, and streamline the user experience.

6.1.16.3. Initial Integration shall include connecting each Customer to the state Cybersecurity Operations Center (CSOC) and validating with FL[DS] that all Solution data is properly integrated, as requested by the Customer.

Tanium provides the ability to connect each customer to the state Cybersecurity Operations Center (CSOC) and validate with FLDS that all solution data is properly integrated, as requested by the customer. This helps to ensure that the customer's security posture is in line with regulatory requirements and best practices. Tanium offers a secure and efficient method for integrating data from multiple sources into a single pane of glass, providing customers with a unified view of their security posture. The solution allows for customization of the data integration process, so that customers can choose the specific data sources that they wish to integrate and the level of granularity at which they want to view that data.

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

Tanium and its partners provide ongoing maintenance and support to ensure the proper exchange of data between customers and the state Cybersecurity Operations Center. This may require additional integration efforts after the initial deployment to address any issues that may arise. The Contractor is responsible for addressing any concerns that FLDS may have regarding integration issues and ensuring that the solution remains fully integrated and functional. Ongoing communication and collaboration between all parties are essential to maintain the effectiveness and efficiency of the integrated system.

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

The Tanium Platform is hosted in multiple AWS Zones to ensure the customer never loses connectivity to the main console.

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

WWT, Tanium and Foresite accept and will adhere to the SLA consequences listed in Table 1 within RFQ DMS-22/23-157.

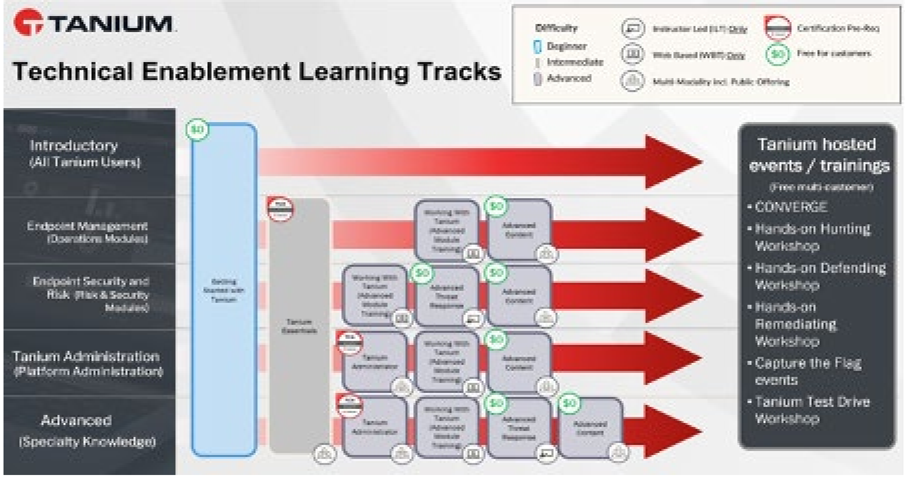
a. A draft SLA for Solution performance and availability which adheres to all provisions of this RFQ.

WWT, Tanium and Foresite accept and will adhere to the SLA consequences listed in Table 1 within RFQ DMS-22/23-157.

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).

WWT, Tanium and Foresite accept and will adhere to the SLA consequences listed in Table 1 within RFQ DMS-22/23-157.

Tanium offers several Enablement Learning Tracks for training as outlined in the diagram below.


TANIUM
Technical Enablement Learning Tracks
Difficulty
Beginner
Intermediate
Advanced
Instructor Led (ILT) Only
Web Based (WBT) Only
Multi-Modality incl. Public Offering
Certification Pre-Req
$0 Free for customers
Introductory (All Tanium Users)
Endpoint Management (Operations Modules)
Endpoint Security and Risk (Risk & Security Modules)
Tanium Administration (Platform Administration)
Advanced (Specialty Knowledge)
Getting Started with Tanium
Tanium Essentials
Working With Tanium (Advanced Module Training)
Advanced Content
Advanced Threat Response
Tanium Administrator
Tanium hosted events / trainings
(Free multi-customer)
• CONVERGE
• Hands-on Hunting Workshop
• Hands-on Defending Workshop
• Hands-on Remediating Workshop
• Capture the Flag events
• Tanium Test Drive Workshop

For Initial Training, Tanium would recommend the following two courses:

- For casual users - Getting Started with Tanium course
- For Admin users (those who will be responsible for administering the system and day to day use) Tanium Essentials.

For ongoing training, the other training programs shown can be purchased at the Customers discretion based on business need as they see fit. This would be for established users. For any new hires, Tanium would recommend the Initial training.

In Appendix A, Tanium has included pricing for both initial and ongoing training. In our pricing for ongoing, Tanium has included one Advanced Course per Customer per year. Additional courses can be arranged through the Tanium Director for Strategic Accounts, but their costs are not included as part of the Pricing in Appendix A. Tanium is happy to collaborate with each customer in the planning stage of their implementation and review the included training, as well as add additional training if the customer feels this is required.

Tanium does offer a Certification program which users can complete, and which also provides Continuing Education Credits (CEU's). If a Customer wishes to have their staff attain Certification, the pricing for the complete set of courses to become certified has also been provided as an option.

Tanium's standard training programs are delivered in multiple modality options:

- **Web Based Training**
    - On-demand
    - Self-paced
    - Targeted at the Individual level
    - Note: Course completion is solely the responsibility of the User
- **Instructor-Led (Virtual Classroom)**
    - Dedicated to customer OR also available as a public course
    - Targeted at a Team or an individual
    - Public courses offered on a monthly basis
    - Course participation and completion are solely the responsibility of the user
- **Instructor-Led (Onsite)**
    - Expert Instructor dedicated to your team
    - Delivered to up to 20 students
    - Requires 4-6 week's notice for scheduling

Given the timelines in the RFQ, Tanium is recommending that all Training be either Web-based or Virtual Classroom at least for inaugural Customers. In a customer's second year, the Onsite Instructor-Led Courses can be of immense value as users know enough to get into more advanced training.

Tanium's standard support model provides a Support Center for Break/Fix responses to Customer initiated tickets. Customers also have the option to purchase support from a Technical Account Manager (TAM). Note: at 25,000 endpoints and above, the TAM cost is discounted to zero; Below 25,000 endpoints, the costs are discounted on a tiered basis as outlined in Appendix A.

Case Severity and Service Levels

The following Service Level Objective (SLO) are goals we strive to achieve, however your contract with Tanium will exclusively govern any contractual obligations in this regard.

Level Description Severity

- 1 - Critical Standard Support (7am – 7pm M-F)
    - Business Hour Response Objective
    - Premium Support (7am - 7pm M-F: All Issue Severities) (24/7: Severity 1 and 2 Issues Only) 1 Hour Response Objective
    - A Severity 1 issue is characterized by the following:
        - An issue which renders Licensed Software inoperative or causes Licensed Software to fail catastrophically
        - An issue where Licensed Software causes business critical applications to malfunction
- Severity 2 – High Standard Support (7am – 7pm M-F)
    - 2 Business Hour Response Objective
    - Premium Support (7am - 7pm M-F: All Issue Severities) (24/7: Severity 1 and 2 Issues Only)
    - 2 Hour Response Objective

- A Severity 2 issue is characterized by the following:
  - An Issue which substantially degrades the performance of Licensed Software or materially restricts use of the Licensed Software
  - Licensed Software experiences instability caused by frequent interruptions
- Severity 3 - Medium Standard Support (7am – 7pm M-F)
  - 8 Business Hour Response Objective
  - Premium Support (7am - 7pm M-F: All Issue Severities) (24/7: Severity 1 and 2 Issues Only)
  - 8 Hour Response Objective
  - A Severity 3 issue is characterized by the following:
    - An Error that causes only a minor impact on the performance of Licensed Software or Customer's use of Licensed Software
    - General usage questions regarding use of Licensed Software

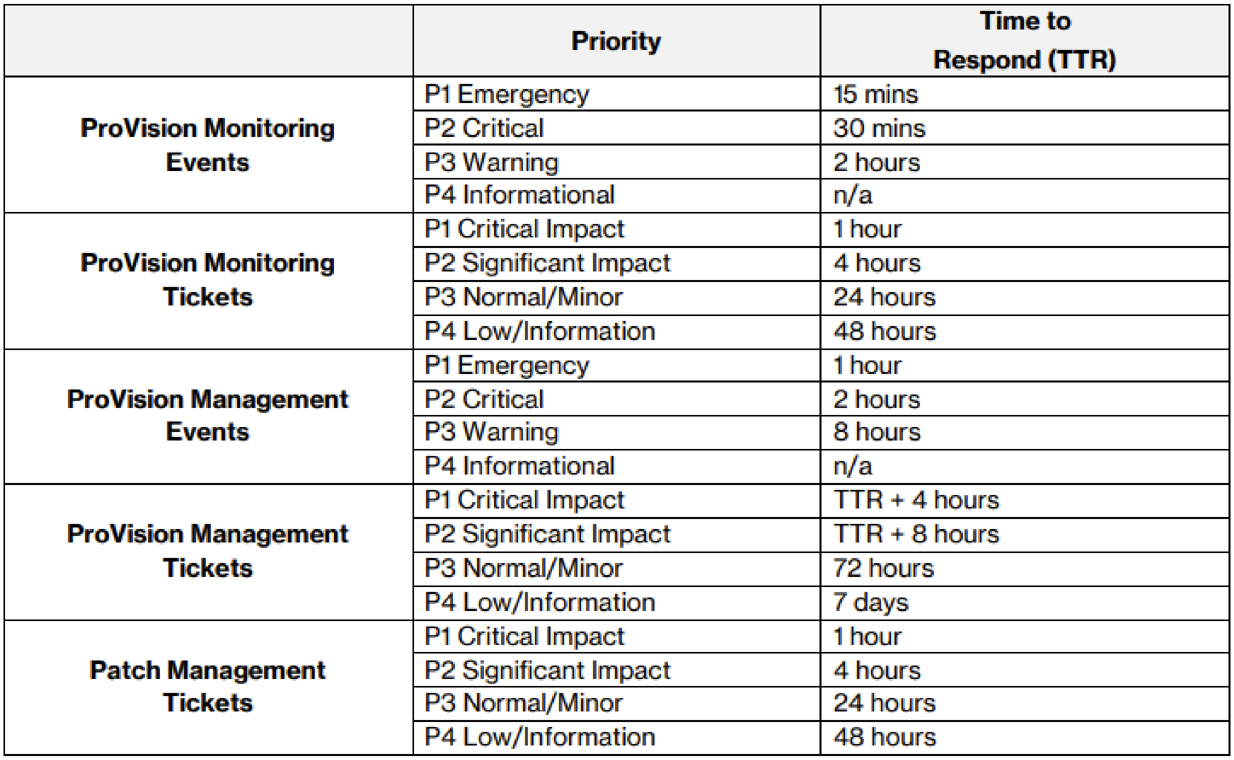
When you open a new support case, support evaluates the severity of your issue using the Tanium Case Severity definitions above.

a. A draft SLA for Solution performance and availability which adheres to all provisions of this RFQ.
WWT, Tanium and Foresite accept and will adhere to the SLA consequences listed in Table 1 within RFQ DMS-22/23-157.

The proposed solution's cloud infrastructure is architected to be in multiple Amazon Web Service (AWS) Zones to provide the SLA percentages that the State of Florida is requiring.

Foresite

The Foresite SLA Matrix is below.



	Priority	Time to Respond (TTR)
ProVision Monitoring Events	P1 Emergency	15 mins
	P2 Critical	30 mins
	P3 Warning	2 hours
	P4 Informational	n/a
ProVision Monitoring Tickets	P1 Critical Impact	1 hour
	P2 Significant Impact	4 hours
	P3 Normal/Minor	24 hours
	P4 Low/Information	48 hours
ProVision Management Events	P1 Emergency	1 hour
	P2 Critical	2 hours
	P3 Warning	8 hours
	P4 Informational	n/a
ProVision Management Tickets	P1 Critical Impact	TTR + 4 hours
	P2 Significant Impact	TTR + 8 hours
	P3 Normal/Minor	72 hours
	P4 Low/Information	7 days
Patch Management Tickets	P1 Critical Impact	1 hour
	P2 Significant Impact	4 hours
	P3 Normal/Minor	24 hours
	P4 Low/Information	48 hours

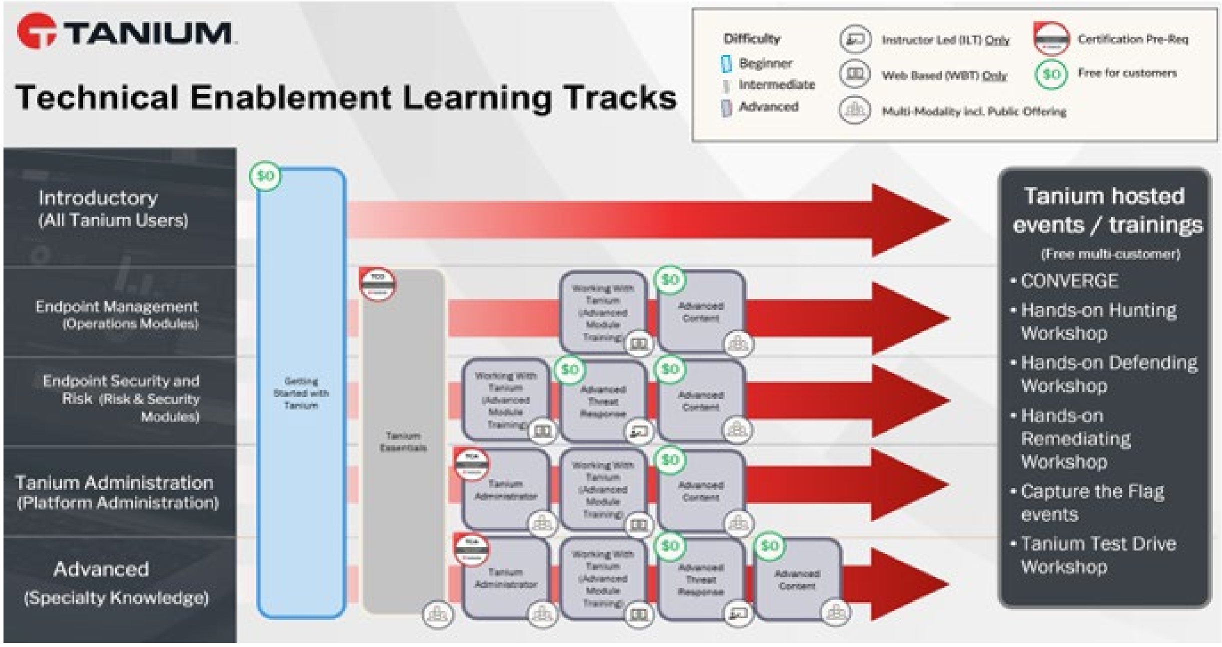
b. A draft SLA for training and support which adheres to all provisions of this RFQ.
i. The training SLA must specify initial training (included in Item No. 1 on Attachment A, Price Sheet) provided and ongoing training provided (included in Item No. 2 on Attachment A, Price Sheet).
WWT, Foresite, Fortinet, Tenable and Elastic accept and will adhere to the SLA consequences listed in FL[DS] – RFQ DMS-22/23-157.

Foresite

The Foresite onboarding team provides initial training directly towards the end of the onboarding/implementation process. During ongoing services, the delivery team (The SOC) will maintain a regular scheduled standing meeting, up to twice a month, to provide access for questions and ongoing training.

Tanium

Tanium offers several Enablement Learning Tracks for training as outlined in the diagram below.



For Initial Training, Tanium would recommend the following two courses:

- For casual users - Getting Started with Tanium course
- For Admin users (those who will be responsible for administering the system and day to day use) - Tanium Essentials.

For ongoing training, the other training programs shown can be purchased at the Customers discretion based on business need as they see fit. This would be for established users. For any new hires, Tanium would recommend the Initial training.

In Attachment A, Tanium has included pricing for both initial and ongoing training. In our pricing for ongoing, Tanium has included one Advanced Course per Customer per year. Additional courses can be arranged through the Tanium Director for Strategic Accounts, but their costs are not included as part of the Pricing in Attachment A. Tanium is happy to collaborate with each customer in the planning stage of their implementation and review the included training, as well as add additional training if the customer feels this is required.

Tanium does offer a Certification program which users can complete, and which also provides Continuing Education Credits (CEU's). If a Customer wishes to have their staff attain Certification, the pricing for the complete set of courses to become certified has also been provided as an option.

Tanium's standard training programs are delivered in multiple modality options:

- Web Based Training
  - On-demand
  - Self-paced
  - Targeted at the Individual level
  - Note: Course completion is solely the responsibility of the User
- Instructor-Led (Virtual Classroom)
  - Dedicated to customer OR also available as a public course
  - Targeted at a Team or an individual
  - Public courses offered on a monthly basis
  - Course participation and completion are solely the responsibility of the user
- Instructor-Led (Onsite)
  - Expert Instructor dedicated to your team
  - Delivered to up to 20 students
  - Requires 4-6 weeks' notice for scheduling

Given the timelines in the RFQ, Tanium is recommending that all Training be either Web-based or Virtual Classroom at least for inaugural Customers. In a customer's second year, the Onsite Instructor-Led Courses can be of immense value as users know enough to get into more advanced training.

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

World Wide Technology

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

Tanium implementations for each customer shall leverage the following high level Implementation Plan. Based on the makeup of each customer's environment and size, WWT reserves the right to adjust the duration section of this plan accordingly, i.e., duration of project may be longer for larger entities.

Where appropriate, WWT has identified components that are the customer's responsibility. Failure on the part of the customer to complete these tasks fully or in a timely manner shall result in a waiver of financial consequences to WWT for activities related to this customer.

A detailed project task list will be shared with each customer during the planning stages of their project along with assigned activities for the customer project team members.

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

Team Definitions	
Teams Defined	FL[DS] Service Experience Team FL[DS] Cyber Operations Team Tanium Sales Tanium TAM WWT Sales WWT Implementation Foresite Team
Groups Defined	**Pre-Sales Team:** • FL[DS] Service Experience Team • WWT Sales • Tanium Sales **Implementation Team:** • FL[DS] Service Experience Team • WWT Sales • Tanium Sales • WWT Implementation Team • Tanium TAM **Post Implementation Team:** • FL[DS] Service Experience Team • WWT Sales • Tanium Sales • Tanium TAM • Foresite

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: • Demonstrations to drive interest. • Technical Q&A sessions to provide answers to any outstanding questions.	Lead: • FL[DS] Service Experience Team • WWT Sales • Tanium Sales
FL[DS] Questionnaire	Review and complete the FL[DS] questionnaire	Lead: • Customer

	Review completed questionnaire and mark agency as "READY"	Lead: • 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 deployment.

Implementation Activities and Tasks		
Call Schedule	Schedule a series of calls for implementation	Lead: • FL[DS] Service Experience Team Included: • WWT PM
Call One Estimated Duration: 60 Minutes	Walk through implementation steps: a) Configuration Needs i) Review FW rules, AV exclusions, others b) Change Management process c) Key Agency Contacts (see examples below) i) SSO Administrator ii) FW Administrator iii) Security Administrator d) Deployment schedule small test group, larger test group, full roll out	Lead: • Implementation Team Include: • Tanium TAM • Foresite Team • FL[DS] Service Experience Team
Call Two Estimated Duration: 30 Minutes	Configure and Troubleshoot Tanium, if necessary	Lead: • FL[DS] Cyber Operations Team Include: • Implementation Team • Tanium TAM
Learning Sessions (Up to 4 Sessions) Estimated Duration: 60 Minutes Each	Conduct Four Learning Sessions: • One Tanium Overview and Basic Tutorial • One Intermediate Tutorial • Two Advanced Tutorials • Implementation Team to discuss with customer meeting scheduling and flow.	Lead: • Implementation Team Include: • FL[DS] Service Experience Team

	- No more than 4 learning sessions total per week	
Deploy Test Group	Test Group Deployment (per agency)	Lead: - WWT Implementation Team Include: - Implementation Team
Call Three Estimated Duration: 30 Minutes	Review rollout to test group, troubleshoot. Deploy to larger test group or schedule another 30-minute call to let trouble shooting take effect and then deploy to larger test group	Lead: - Tanium TAM Include: - Post Implementation Team
Call Four Estimated Duration: 60 Minutes	Review results and impact of larger group deployment, trouble shoot and setup full deployment.	Lead: - Tanium TAM Include: - Post Implementation Team
Call Five Estimated Duration: 60 Minutes	Managed Services Onboarding	Lead: - Foresite Include: - Post Implementation Team
Call Six Estimated Duration: 60 Minutes	Review full deployment, platform overview	Lead: - Tanium TAM/FL[DS] Service Experience Include: - Foresite
Call Seven Estimated Duration: 30 - 60 Minutes	Tanium-specific Call - Walk through any outstanding features/capabilities required for the solution	Lead: - Tanium TAM/FL[DS] Service Experience Include: - Foresite
Call Eight	Review full deployment:	Lead:

Estimated Duration: 60 Minutes	• Discuss progress • Close any open items • Identify and address gaps in solution	• FL[DS] Services Experience Include: • WWT Sales • Tanium Sales • Foresite Team • Implementation Team

Implementation Activities and Tasks		
Individual Agency Calls Estimated Duration: 30 - 60 Minutes	Per agency value calls	Lead: • FL[DS] Services Experience Include: • WWT Sales • Tanium Sales • Foresite Team

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

WWT and Foresite accept and will adhere with the SLA consequences listed in FL[DS] – RFQ DMS-22/23-157.

Foresite
Events

Priority	Time to Respond	Target to Address
P1 Emergency	15 mins	1 hour
P2 Critical	30 mins	2 hours
P3 Warning	2 hours	8 hours
P4 Informational	n/a	n/a

Tickets:

Priority	Time to Respond	Target to Resolve
P1 Critical Impact	1 hour	TTR + 4 hours
P2 Significant Impact	4 hours	TTR + 8 Hours
P3 Normal/Minor	24 hours	72 hours
P4 Low/Information	48 hours	7 days

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

WWT, Foresite, and Tanium accept and will adhere with the SLA consequences listed in FL[DS] – RFQ DMS-22/23-157.

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.

Integration Type	SLA Integration Timeline	Hours	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 32.5.
WWT, Foresite and Tanium accept and will adhere with the SLA consequences listed in FL[DS] – RFQ DMS-22/23-157.

World Wide Technology

The solutions proposed for Security Operations Platform Solution RFQ listed below all strive for high availability based on their architectures and processes towards industry standard 99.95% availability yearly and higher. The solution architectures hosted in the cloud platforms allow for higher availability for our customers and disaster recovery by operating across multiple geographical cloud zones. The solutions strive to be always available to enable our customers security and business capabilities.

Our proposed solutions focus on achieving high availability of 99.999% (often referred to as "five nines") and are built with careful planning, architecture design, and implementation.

Some key considerations and strategies we utilize to achieve such high availability are:

- **Redundancy and Fault Tolerance:** Solution designed with redundancy at multiple levels, including hardware, software, and data utilizing techniques such as load balancing, clustering, and replication to ensure that there are multiple instances of critical components, and failures can be automatically detected and handled without impacting the overall availability.

- **Distributed Architecture:** Solution distributed across multiple physical or virtual servers in different locations. This helps to mitigate the risk of a single point of failure and enables load balancing and failover mechanisms.

- **Automatic Failover**: Solution automated failover mechanisms to detect failures and switch to backup or redundant systems seamlessly.

- **Monitoring and Alerting:** Solution employs comprehensive monitoring systems to track the performance, availability, and health of the application and its underlying infrastructure.

- **Scalability with Foresite and Tanium:** Solution designed to scale horizontally by adding more resources or instances to handle increased load.

- **Isolation and Microservices:** Solution utilizes a microservices architecture where different components or services are decoupled and run independently. This allows for easier scalability, fault isolation, and independent deployment and updates, minimizing the impact of failures or changes on the overall system.

- **Backup and Disaster Recovery**: Solution has regular backups and robust disaster recovery mechanisms.

- **Geographical Redundancy:** Solution has geographical redundancy by deploying application instances in different regions or data centers.

- **Continuous Deployment and Testing:** Solution development embraces continuous integration, continuous deployment (CI/CD) practices, and thorough automated testing.

- **Robust Infrastructure:** Solution is architected in a reliable and high-performance infrastructure and utilizes cloud-based services or infrastructure-as-a-service (IaaS) providers that offer built-in redundancy and high availability features.

Foresite

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.

Foresite maintains two, regionally diverse, SOCs as BCDR, and the ability, as a last resort, to allow our analysts to work remotely in the even both SOCs are impacted and are unreachable.

Tanium

Tanium has a BCP/DR Policy that is exercised routinely and, as part of our Information Security Management System (ISMS), it is regularly audited by our external auditors, including ISO27001.

Tanium’s infrastructure is found in multiple AWS Zones to prevent outages in services to their customers.

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

Project # 1: Large Healthcare Provider

Challenge

A WWT Customer with a large quantity of facilities around the country, needed to deploy the Tanium agent and all modules to their HQ and to all endpoint locations. These locations suffered from low bandwidth issues and were sensitive in nature due to the company’s vertical.

Approach

The customer reached out to WWT to build a WWT Tanium Services engagement around this activity. WWT’s team of SMEs developed a robust program plan to tackle each location in an accelerated timeframe. This plan ensured sensitive endpoints were protected from impact and unique scenarios were addressed. The deployment was based on a 20%, 50%, 70%, 100%, Sensitive/Critical rollout for tools and changes. This breakdown allowed for through assessment of each endpoint category, as well as providing remote locations the comfort of knowing proper testing had been completed.

Benefits

The deployment of agents and modules to all endpoints (>150,000) was completed in record time per our Tanium partner. This was the quickest deployment of these tools in Tanium's history. Functionality was given to the customer's team to better protect their environment and provide visibility to remote endpoints they have not previously been able to manage.

Project # 2: Large Federal Customer

Challenge

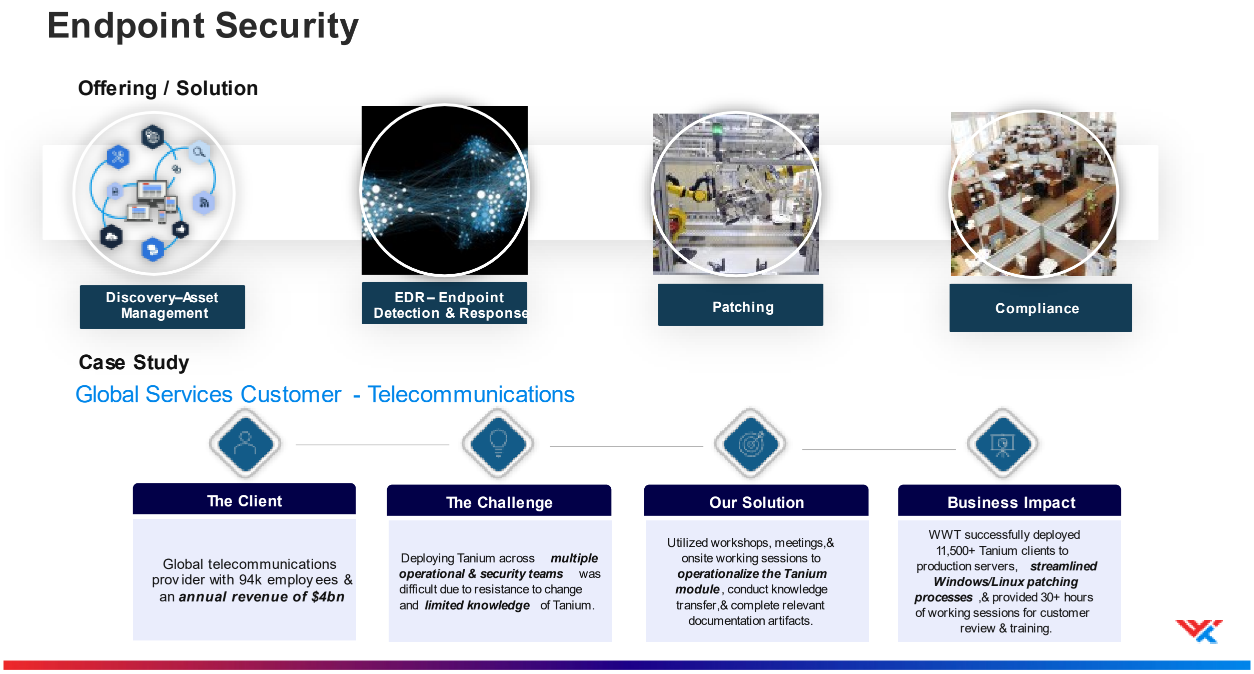
The federal customer needed help implementing and managing Tanium across their vast environment of over a million endpoints to gain visibility, discovery, as well as increase security posture thru patching and compliance.

Approach

WWT managed the large U.S. Federal customer with the Tanium solution for three years with WWT resources all around the world implementing and supporting the Tanium solution. WWT sped up deployments of the Tanium solution and agents across this customer's million endpoints. Based on the Tanium data the customer observed, WWT helped execute actions to patch endpoints at speed and scale to reduce risk to the environment. WWT also drove implementing and measuring compliance on endpoints and recommending any remediations needed to bring those systems back into compliance. WWT worked hand in hand with Tanium with this customer and have created multiple integrations to other tools in customer's environments such as Cisco ISE, Splunk, and more.

Benefits

The customer with WWT implementing and supporting Tanium was able to increase visibility, improve patching, increase their security posture, and ensure compliance on over a million endpoints globally. WWT was able to train the customer operators of Tanium to find the data to make decisions State of Florida across their large environment. WWT also produced Tanium module runbooks and documentation to run the Tanium platform incorporating best practices.



Endpoint Security

Offering / Solution

Discovery–Asset Management
EDR – Endpoint Detection & Response
Patching
Compliance

Case Study

Global Services Customer - Telecommunications

The Client

Global telecommunications provider with 94k employees & an ***annual revenue of $4bn***

The Challenge

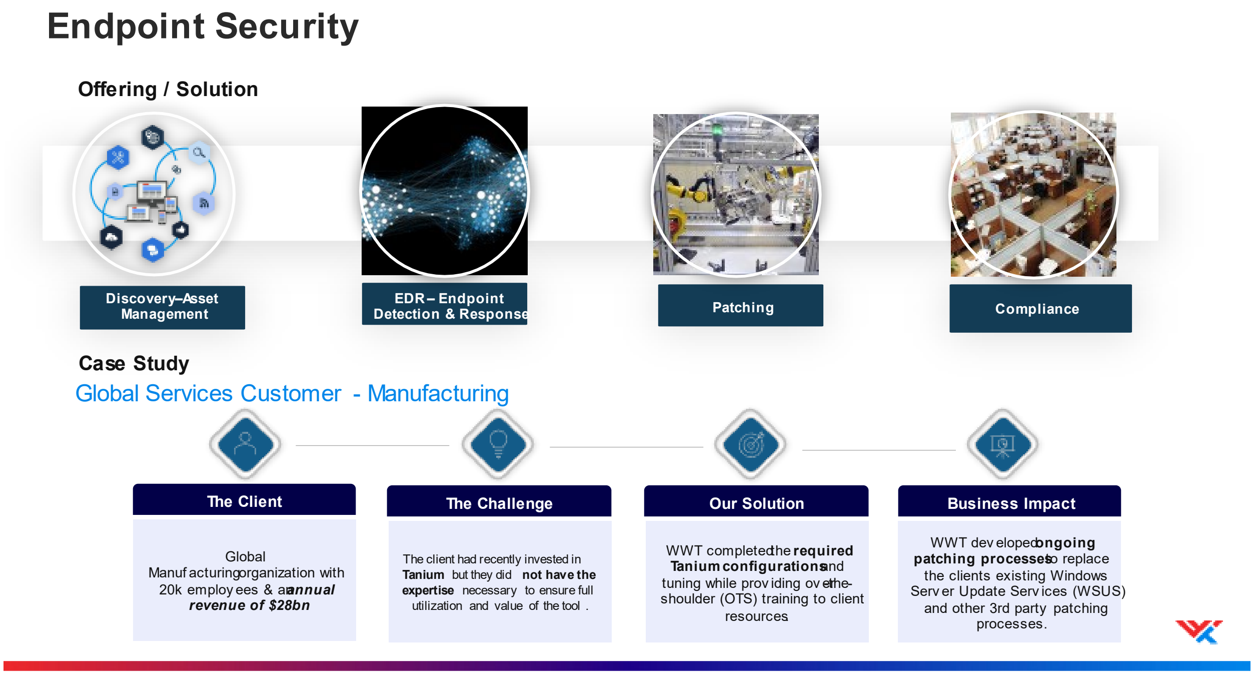
Deploying Tanium across ***multiple operational & security teams*** was difficult due to resistance to change and ***limited knowledge*** of Tanium.

Our Solution

Utilized workshops, meetings,& onsite working sessions to ***operationalize the Tanium module***, conduct knowledge transfer,& complete relevant documentation artifacts.

Business Impact

WWT successfully deployed 11,500+ Tanium clients to production servers, ***streamlined Windows/Linux patching processes*** ,& provided 30+ hours of working sessions for customer review & training.



Endpoint Security

Offering / Solution

Discovery–Asset Management
EDR – Endpoint Detection & Response
Patching
Compliance

Case Study

Global Services Customer - Manufacturing

The Client

Global Manufacturing organization with 20k employees & an ***annual revenue of $28bn***

The Challenge

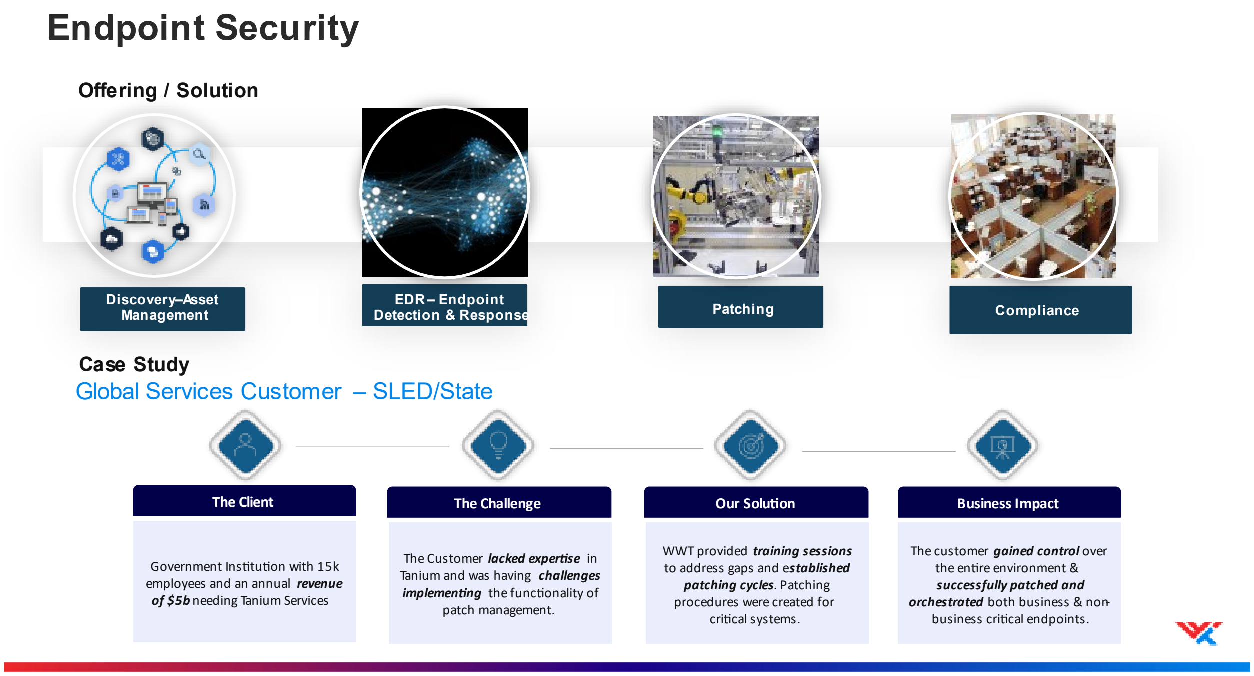
The client had recently invested in **Tanium** but they did **not have the expertise** necessary to ensure full utilization and value of the tool .

Our Solution

WWT completed the **required Tanium configurations** and tuning while providing over-the-shoulder (OTS) training to client resources.

Business Impact

WWT developed **ongoing patching processes** to replace the clients existing Windows Server Update Services (WSUS) and other 3rd party patching processes.



Endpoint Security

Offering / Solution

Discovery–Asset Management

EDR – Endpoint Detection & Response

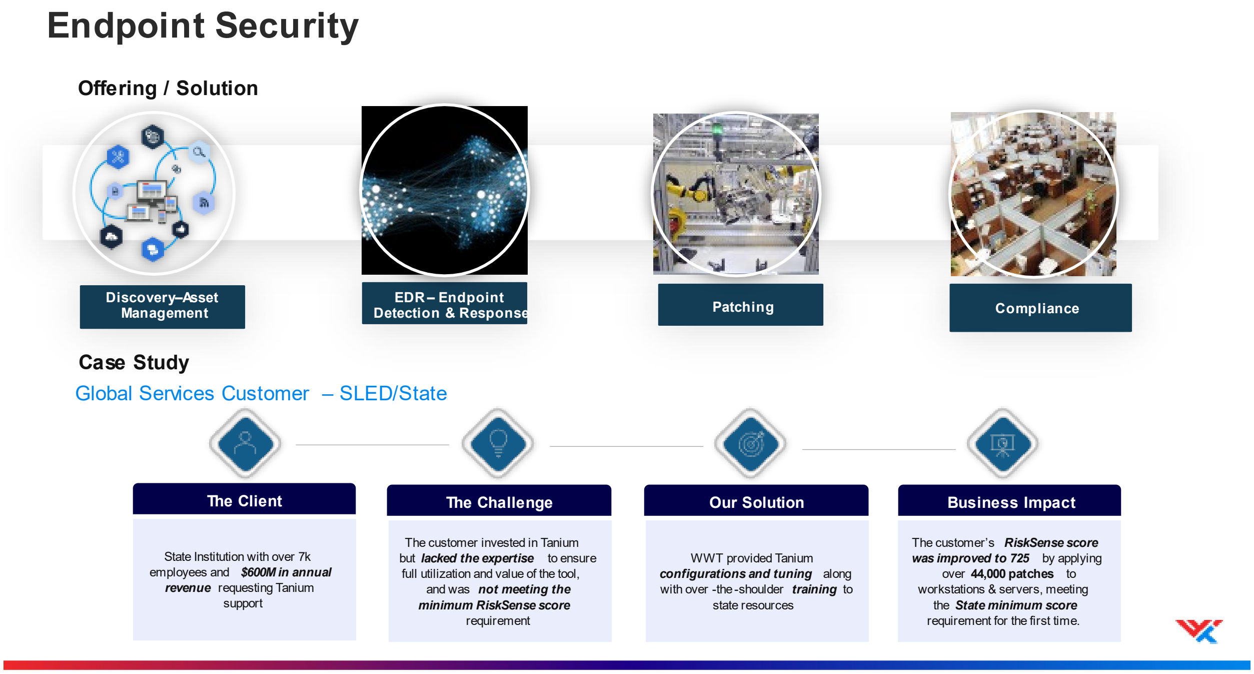
Patching

Compliance

Case Study

Global Services Customer – SLED/State

The Client	The Challenge	Our Solution	Business Impact
Government Institution with 15k employees and an annual ***revenue of $5b*** needing Tanium Services	The Customer ***lacked expertise*** in Tanium and was having ***challenges implementing*** the functionality of patch management.	WWT provided ***training sessions*** to address gaps and e***stablished patching cycles***. Patching procedures were created for critical systems.	The customer ***gained control*** over the entire environment & ***successfully patched and orchestrated*** both business & non-business critical endpoints.



Endpoint Security

Offering / Solution

Discovery–Asset Management

EDR – Endpoint Detection & Response

Patching

Compliance

Case Study

Global Services Customer – SLED/State

The Client	The Challenge	Our Solution	Business Impact
State Institution with over 7k employees and ***$600M in annual revenue*** requesting Tanium support	The customer invested in Tanium but ***lacked the expertise*** to ensure full utilization and value of the tool, and was ***not meeting the minimum RiskSense score*** requirement	WWT provided Tanium ***configurations and tuning*** along with over -the-shoulder ***training*** to state resources	The customer's ***RiskSense score was improved to 725*** by applying over **44,000 patches** to workstations & servers, meeting the ***State minimum score*** requirement for the first time.

Foresite Cybersecurity has been performing Managed Security Services that include Tanium management and monitoring, external, internal, wireless and physical network security scanning and other Managed Security Services for over 10 years. On average we perform 250 engagements per year for scanning and testing services. This includes providing managed Tanium services for FL[DS].

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

WWT is driving implementation and operationalization of the Tanium solution for the State of Florida per the RFP DMS-21/22-240 Asset Discovery Software and Support over the last year. We have been working with the Tanium, Foresite, the State of Florida, and State of Florida agency teams to deploy the Tanium solution to thousands of endpoints at scale and speed to provide visibility, gain control over the environment and critical endpoints and increase security maturity for the State of Florida. WWT also provided training sessions for multiple Tanium modules to drive adoption.

Our WWT Program Management capabilities and collaboration with multiple groups has enabled us to pull in resources to scale, meet project timelines and deliver with excellence. The WWT team has utilized many templates and documents from prior engagements around the program management and security solutions for the Department and its customers to optimize implementation times and reduce resource requirements and meetings.

4) Detail regarding any value-added services.

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.

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

Google Cloud
aws
ATC
EQUINIX

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

Tanium Value Added Services

- **Complimentary Training**
  - **Getting Started w/Tanium:** This course introduces the Tanium platform's unique architecture and benefits, along with the key functionality of its Core modules, including asking questions, analyzing data, and connecting with external destinations. You will also receive a brief preview of additional Tanium modules available to support more advanced Endpoint Management and Endpoint Risk & Security use cases.
  - Tanium is happy to provide a variety of complimentary training aligned to specific purchases.
  - Tanium is happy to provide complimentary Converge (user conference tickets/labs) aligned to specific purchases.

- **Support Resources**
  - **Client Engagement Specialist-** Tanium's Client Engagement Specialists play a vital role in fostering strong relationships and effective communication with customers. Serving as the primary point of contact, they actively listen to customer needs, address inquiries, and provide tailored solutions. These specialists collaborate with internal teams to ensure smooth onboarding, implementation, and support throughout the customer journey. By understanding customer goals and challenges, they offer insights, guidance, and best practices to maximize the value of Tanium's offerings. Proactive engagement, regular check-ins, and business reviews help assess satisfaction levels and identify areas for improvement, while advocating for customer feedback within Tanium. Client Engagement Specialists at Tanium act as trusted advisors, building partnerships and ensuring customer success. Their focus on personalized support, effective communication, and customer satisfaction contributes to a positive and productive

customer experience. Contact information will be provided to the customer entity during implementation.

- **Whole of State Support:** With deep knowledge and experience in working with state governments, Tanium offers tailored solutions and services that align with specific regulatory frameworks, security standards, and operational needs. By combining advanced technology, best practices, and industry expertise, Tanium helps state governments optimize IT operations, enhance cybersecurity, and streamline management across their entire infrastructure, providing holistic and effective solutions for the complex landscape of state-level governance.

- **State Designated Engineer:**
  A State Designated Engineer will help facilitate onboarding, implementation, best practice sharing, and value delivery. They leverage their technical expertise to align customer requirements with Tanium's and FL[DS]' capabilities. From supporting the initial setup to offering recommendations on best practices, they ensure a smooth integration. Collaborating with various stakeholders, they drive successful adoption and maximize customer satisfaction, contributing to long-term value delivery. Contact information will be provided to the customer entity during implementation.

- **Integrations**
  Integration with other systems: Tanium is a comprehensive endpoint security and management platform that offers powerful integration capabilities. Tanium Connect enables seamless integration between Tanium and other enterprise systems, allowing organizations to consolidate their security and IT operations workflows. With Tanium Connect, users can establish bidirectional communication with various tools, such as SIEMs, IT service management platforms, and ticketing systems. This integration empowers organizations to leverage existing investments in security and IT infrastructure, streamline processes, and enhance their overall security posture. By connecting Tanium with other systems, users gain a holistic view of their environment and can take informed actions to respond quickly and effectively to security threats and operational challenges.

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

All pricing on the Attachment A, Price Sheet, are Not-To-Exceed (NTE) pricing. Final pricing will be negotiated once the size of the entities is discussed.

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

6) 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.

7) 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.

WWT, Foresite, Fortinet, Tenable and Elastic accept and will adhere with the SLA consequences listed in FL[DS] – RFQ DMS-22/23-157.

Foresite

ProVision Optional Modules*

Patch Management

- ProVision Patch Management Service (Workstation)
- ProVision Patch Management Service (Server)

Managed Detection & Response (MDR)

- ProVision Managed Detection & Response (MDR) (No License)
- **ProVision Managed Detection & Response (MDR) + CrowdStrike MSSP Defend Bundle
- **ProVision Managed Detection & Response (MDR) + CrowdStrike MSSP Advanced Defend Bundle

Automated Breach & Attack Simulation + Red Team Services

- Automated Breach and Attack Simulation+ Red Team Services

Firewall Management

- ProVision Firewall Management (Small)
- ProVision Firewall Management (Standard)
- ProVision Firewall Management (Enterprise)

Additional details on these optional ProVision modules can be found attached, ***Foresite ProVision Service Description***.

*Optional modules require ProVision Essential or ProVision Elite
**CrowdStrike pricing is available for organizations up to 2,500 endpoints. Manufacture authorization and potentially better pricing available for larger organizations.

Option #1

ProVision Essential

- Standard offering
- 24x7x365 Security Operation Center
- Includes ingestion from the supported list, ***Foresite ProVision Portfolio Supported Products***
- Assets are limited by size of the organization using tiers by user count

Product Name	Users	Assets
ProVision Essential - Tier 1	25-50	5
ProVision Essential - Tier 2	51-100	10
ProVision Essential - Tier 3	101-150	15
ProVision Essential - Tier 4	151-200	20

ProVision Essential - Tier 5	201-250	25
ProVision Essential - Tier 6	251-300	35
ProVision Essential - Tier 7	301-500	50
ProVision Essential - Tier 8	501-1,000	100
ProVision Essential - Tier 9	1,001-1,500	150
ProVision Essential - Tier 10	1,501-2,000	200
ProVision Essential - Tier 11	2,001-3,000	300
ProVision Essential - Tier 12	3,001-4,000	350
ProVision Essential - Tier 13	4,001-5,000	450
ProVision Essential - Tier 14	5,001+	Custom

- Incident Response Support

Option #2

ProVision Elite

- 24x7x365 Security Operation Center
- Powered by Google Chronicle
- Includes ingestion from the supported list (https://cloud.google.com/chronicle/docs/ingestion/parser-list/supported-default-parsers)
- SOAR
- MITRE ATT&CK Framework alignment
- AI/Machine Learning
- Threat Hunting
- Incident Response Support
- Unlimited corporate telemetry

ProVision Platform

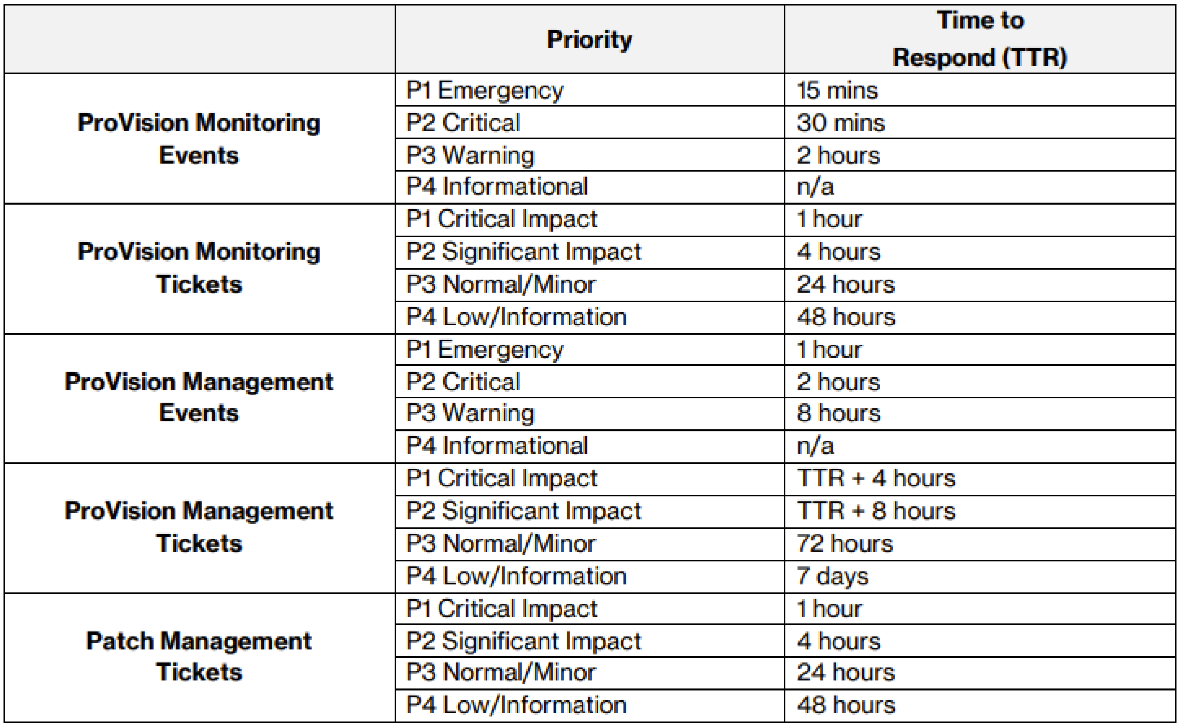
Foresite has developed their own proprietary multi-tenant Managed Security Services Platform, ProVision, and has all the design, development, and implementation resources in-house. The solution infrastructure is hosted on AWS, giving the platform the scalability, flexibility, and performance to exceed 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 NIST 800-53, NIST-CSF, Cyber Essentials +, PCI Gap Analysis, Cloud Security Posture, vCISO and more.

Foresite has been active as a Managed Security Service Provider (MSSP) since 2013. 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 is ISO:27001 certified and the datacenter is SOC 1&2 compliant.

The Foresite SLA Matrix is below.



	Priority	Time to Respond (TTR)
ProVision Monitoring Events	P1 Emergency	15 mins
	P2 Critical	30 mins
	P3 Warning	2 hours
	P4 Informational	n/a
ProVision Monitoring Tickets	P1 Critical Impact	1 hour
	P2 Significant Impact	4 hours
	P3 Normal/Minor	24 hours
	P4 Low/Information	48 hours
ProVision Management Events	P1 Emergency	1 hour
	P2 Critical	2 hours
	P3 Warning	8 hours
	P4 Informational	n/a
ProVision Management Tickets	P1 Critical Impact	TTR + 4 hours
	P2 Significant Impact	TTR + 8 hours
	P3 Normal/Minor	72 hours
	P4 Low/Information	7 days
Patch Management Tickets	P1 Critical Impact	1 hour
	P2 Significant Impact	4 hours
	P3 Normal/Minor	24 hours
	P4 Low/Information	48 hours

Managed Detection and Response (MDR)

Foresite Cybersecurity's MDR Services provide better proactive defense than traditional managed security services alone. Foresite's MDR solutions enable a proactive and advanced approach to cybersecurity. Advanced detection of malicious activities through security threat hunting and monitoring significantly reduce days to response, and rapid incident analysis and response significantly lessons security breach costs.

Foresite will utilize EDR technology to investigate devices and network data within the organizations infrastructure to attempt to identify malicious and/or suspicious activity.

Using pro-active threat hunting techniques, the service is designed to uncover advanced threats potentially hiding within the organization.

Managed Detection and Response service features:

- EDR Software / Licensing

- Threat Hunting
- ProVision Platform integration
- First Line Support/Management of the EDR
- 24x7x365 monitoring
- Policy development and management
- Custom Watchlist Alerting
- Advance Reporting
- Proactive Response

Service Scope

Foresite's MDR service provides real-time security monitoring, analysis and identification of potential areas of compromise within the Client's estate. On top of managing the EDR platform, Foresite will proactively hunt the Client's estate for potentially hidden threats, known vulnerabilities, potential misconfigurations, and recommend policy tuning.

All Foresite activities are unobtrusive and conducted in the background with the customer only being alerted should a threat and/or vulnerability be discovered. Identified and potential threats will be logged as Security Incident Tickets and progressed/mitigated as per the section above on Ticketing.

Threat Hunting	Foresite will run Threat Hunting sessions across the Client's estate that includes information gathering, searches across the customer estate, and the generation of the automation/watchlist.
Automation	Foresite will add all manual hunts, where possible, into an automated process. This will enable alerting and a better security posture on the latest threats.

Onboarding Stages:

Sensor Rollout	Foresite will provide the installation package for distribution to the endpoint sensors onto all Devices/Assets.
Policy Implementation	Foresite recommended policies are put in place that include individual policies for Standard Endpoints, High-value Endpoints, Standard Servers, Mission Critical Servers.
Tuning	Data and Alerts will be reviewed and tuning recommended based on Threat Hunting results, false positive alerts, customer requirements.

Tanium Value Added Services

- **Complimentary Training**
  - **Getting Started w/Tanium:** This course introduces the Tanium platform's unique architecture and benefits, along with the key functionality of its Core modules, including

asking questions, analyzing data, and connecting with external destinations. You will also receive a brief preview of additional Tanium modules available to support more advanced Endpoint Management and Endpoint Risk & Security use cases.
    - Tanium is happy to provide a variety of complimentary training aligned to specific purchases.
    - Tanium is happy to provide complimentary Converge (user conference tickets/labs) aligned to specific purchases.

- **Support Resources**
    - **Client Engagement Specialist-** Tanium's Client Engagement Specialists play a vital role in fostering strong relationships and effective communication with customers. Serving as the primary point of contact, they actively listen to customer needs, address inquiries, and provide tailored solutions. These specialists collaborate with internal teams to ensure smooth onboarding, implementation, and support throughout the customer journey. By understanding customer goals and challenges, they offer insights, guidance, and best practices to maximize the value of Tanium's offerings. Proactive engagement, regular check-ins, and business reviews help assess satisfaction levels and identify areas for improvement, while advocating for customer feedback within Tanium. Client Engagement Specialists at Tanium act as trusted advisors, building partnerships and ensuring customer success. Their focus on personalized support, effective communication, and customer satisfaction contributes to a positive and productive customer experience.

    - **Whole of State Support:** With deep knowledge and experience in working with state governments, Tanium offers tailored solutions and services that align with specific regulatory frameworks, security standards, and operational needs. By combining advanced technology, best practices, and industry expertise, Tanium helps state governments optimize IT operations, enhance cybersecurity, and streamline management across their entire infrastructure, providing holistic and effective solutions for the complex landscape of state-level governance.

    - **State Designated Engineer:**
      A State Designated Engineer will help facilitate onboarding, implementation, best practice sharing, and value delivery. They leverage their technical expertise to align customer requirements with Tanium's and FL[DS]' capabilities. From supporting the initial setup to offering recommendations on best practices, they ensure a smooth integration. Collaborating with various stakeholders, they drive successful adoption and maximize customer satisfaction, contributing to long-term value delivery.

    - **Integrations**
      Integration with other systems: Tanium is a comprehensive endpoint security and management platform that offers powerful integration capabilities. Tanium Connect enables seamless integration between Tanium and other enterprise systems, allowing organizations to consolidate their security and IT operations workflows. With Tanium Connect, users can establish bidirectional communication with various tools, such as SIEMs, IT service management platforms, and ticketing systems. This integration empowers organizations to leverage existing investments in security and IT infrastructure, streamline processes, and enhance their overall security posture. By

connecting Tanium with other systems, users gain a holistic view of their environment and can take informed actions to respond quickly and effectively to security threats and operational challenges.

World Wide Technology

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
___X__ 43230000-NASPO-16-ACS Cloud Solutions
______ 43230000-23-NASPO-ACS Software Value Added Reseller (SVAR)

II. Pricing Instructions

The vendor shall provide fixed rates quoted at or below the rates in the applicable ACS contract selected in Section I above. 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

Below are the pricing table for different bundles of Tanium. All prices are not-to-exceed (NTE) pricing. All tables are based on Tanium Core, Asset, and Discover Modules. For other bundle options and waterfall pricing modules available to the State of Florida, please go to Section V. of this document.

Training for 1 year to Tanium's Essentials Virtual Training is provided to each administrator at no cost as shown in each of the following breakdowns that fall under the FL[DS] umbrella. If a Customer Entity wants to purchase on their own and in a standalone fashion, the training will need to be purchased at $8,647.96 for the initial person, and then $306.12 for each additional person. All names must be given at the start of the training subscription to receive the add-on price.

Pricing for Customer Entity under Florida CSOC

This pricing is for Tanium Software and Implementation only. Pricing is only permitted if the customer entity is under the Florida CSOC.

Bundle 1: Tanium Modules: Core Suite, Threat Response, and Impact

Implementation and Licensing
Tanium Modules: Core, Threat Response, and Impact
Initial Term Pricing (Years 1-3)

Item No.	Description	Rate Per Device/Endpoint
1	**Initial Software Year** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$25.28 - 125,000 to 249,999 $24.20 - 250,000 to 374,999 $23.17 - 375,000 to 499,999 $22.18 - 500,000+
2	**Subsequent Software Year** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$20.52 - 125,000 to 249,999 $19.49 - 250,000 to 374,999 $18.52 - 375,000 to 499,999 $17.59 - 500,000+

Implementation and Licensing
Tanium Modules: Core, Threat Response, and Impact
Renewal Term Pricing (Years 4-6) (Optional)

Item No.	Description	Rate Per Device/Endpoint
1	**Renewal Software Year (~15% higher than Year 1)** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$29.08 - 125,000 to 249,999 $27.83 - 250,000 to 374,999 $26.64 - 375,000 to 499,999 $25.21 - 500,000+
2	**Subsequent Software Year (5% increase each year)** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$23.59 - 125,000 to 249,999 $22.41 - 250,000 to 374,999 $21.29 - 375,000 to 499,999 $20.23 - 500,000+

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
Tanium Waterfall Software SKUs			
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 26.75	$ 9.87
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 26.75	$ 9.37
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 26.75	$ 8.90
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Endpoints	$ 26.75	$ 8.46
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 21.00	$ 7.75
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 21.00	$ 7.36
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 21.00	$ 6.99
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 21.00	$ 6.64
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 5.50	$ 2.02
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 5.50	$ 1.92
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 5.50	$ 1.83
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 5.50	$ 1.73
Tanium Training SKUs			

TAN-TRN-VIRTUAL-E	Essentials Virtual 1 yr	$ 16,950.00	$ -
WWT Implementation SKUs			
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 5.65
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 250,000 - 374,999 Endpoints	$ 25,000.00	$ 5.55
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 375,000 - 499,999 Endpoints	$ 25,000.00	$ 5.45
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 500,000+ Endpoints	$ 25,000.00	$ 5.35

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
Tanium Waterfall Software SKUs			
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 26.75	$ 10.85
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 26.75	$ 10.31
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 26.75	$ 9.80
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Endpoints	$ 26.75	$ 9.30
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 21.00	$ 8.52
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 21.00	$ 8.10
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 21.00	$ 7.69
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 21.00	$ 7.31
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 5.50	$ 2.22

TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 5.50	$ 2.11
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 5.50	$ 2.01
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 5.50	$ 1.91
Tanium Training SKUs			
TAN-TRN-VIRTUAL-E	Essentials Virtual 1 yr	$ 16,950.00	$ -

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
Tanium Direct Connect/ScreenMeet			
SS-RMT	Remote Screen Share - 1 required per Customer Entity Administrator to facilitate RFQ Requirement in Section 6.1.16	$ 1,500.00	$ 1,450.50
World Wide Technology Program Management for Managed Services			
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 125,000 - 249,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.21
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 250,000 - 374,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.11
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 375,000 - 499,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.01
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 500,000+ Endpoints Per Endpoint	$ 25,000.00	$ 3.91
World Wide Technology Managed Services			
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 19.71
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 250,000 - 374,999 Endpoints	$ 25,000.00	$ 19.12
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 375,000 - 499,999 Endpoints	$ 25,000.00	$ 18.45

PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 500,000+ Endpoints	$ 25,000.00	$ 17.53

Bundle 2: Tanium Modules: Core Suite, Threat Response, Impact, Patch and Deploy

Implementation and Licensing Tanium Modules: Core, Threat Response, Impact, Patch, and Deploy Initial Term Pricing (Years 1-3)		
Item No.	**Description**	**Rate Per Device/Endpoint**
1	**<u>Initial Software Year</u>** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$31.17 - 125,000 to 249,999 $29.80 - 250,000 to 374,999 $28.48 - 375,000 to 499,999 $27.23 - 500,000+
2	**<u>Subsequent Software Year</u>** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$26.67 - 125,000 to 249,999 $25.34 - 250,000 to 374,999 $24.07 - 375,000 to 499,999 $22.87 - 500,000+

Implementation and Licensing Tanium Modules: Core, Threat Response, Impact, Patch, and Deploy Renewal Term Pricing (Years 4-6) (Optional)		
Item No.	**Description**	**Rate Per Device/Endpoint**
1	**<u>Renewal Software Year (~15% higher than Year 1)</u>** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$35.85 - 125,000 to 249,999 $34.27 - 250,000 to 374,999 $32.76 - 375,000 to 499,999 $31.32 - 500,000+
2	**<u>Subsequent Software Year (5% increase each year)</u>** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$30.67 - 125,000 to 249,999 $29.14 - 250,000 to 374,999 $27.68 - 375,000 to 499,999 $26.30 - 500,000+

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
Tanium Waterfall Software SKUs			
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 26.75	$ 9.87
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 26.75	$ 9.37
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 26.75	$ 8.90
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Endpoints	$ 26.75	$ 8.46
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 21.00	$ 7.75
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 21.00	$ 7.36
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 21.00	$ 6.99
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 21.00	$ 6.64
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 5.50	$ 2.02
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 5.50	$ 1.92
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 5.50	$ 1.83
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 5.50	$ 1.73
TAN-PTCH2-TAAS	Patch Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 8.00	$ 2.95

TAN-PTCH2-TAAS	Patch Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 8.00	$ 2.80
TAN-PTCH2-TAAS	Patch Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 8.00	$ 2.66
TAN-PTCH2-TAAS	Patch Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 8.00	$ 2.52
TAN-DEPLOY-TAAS	Deploy Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 8.00	$ 2.95
TAN-DEPLOY-TAAS	Deploy Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 8.00	$ 2.80
TAN-DEPLOY-TAAS	Deploy Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 8.00	$ 2.66
TAN-DEPLOY-TAAS	Deploy Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 8.00	$ 2.52
Tanium Training SKUs			
TAN-TRN-VIRTUAL-E	Essentials Virtual 1 yr	$ 16,950.00	$ -
WWT Implementation SKUs			
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 5.65
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 250,000 - 374,999 Endpoints	$ 25,000.00	$ 5.55
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 375,000 - 499,999 Endpoints	$ 25,000.00	$ 5.45
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 500,000+ Endpoints	$ 25,000.00	$ 5.35

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
Tanium Waterfall Software SKUs			
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 26.75	$ 10.85

TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 26.75	$ 10.31
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 26.75	$ 9.80
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Endpoints	$ 26.75	$ 9.30
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 21.00	$ 8.52
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 21.00	$ 8.10
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 21.00	$ 7.69
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 21.00	$ 7.31
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 5.50	$ 2.22
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 5.50	$ 2.11
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 5.50	$ 2.01
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 5.50	$ 1.91
TAN-PTCH2-TAAS	Patch Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 8.00	$ 3.24
TAN-PTCH2-TAAS	Patch Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 8.00	$ 3.08
TAN-PTCH2-TAAS	Patch Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 8.00	$ 2.93
TAN-PTCH2-TAAS	Patch Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 8.00	$ 2.78

TAN-DEPLOY-TAAS	Deploy Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 8.00	$ 3.24
TAN-DEPLOY-TAAS	Deploy Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 8.00	$ 3.08
TAN-DEPLOY-TAAS	Deploy Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 8.00	$ 2.93
TAN-DEPLOY-TAAS	Deploy Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 8.00	$ 2.78
Tanium Training SKUs			
TAN-TRN-VIRTUAL-E	Essentials Virtual 1 yr	$ 16,950.00	$ -

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**
Tanium Direct Connect/ScreenMeet			
SS-RMT	Remote Screen Share - 1 required per Customer Entity Administrator to facilitate RFQ Requirement in Section 6.1.16	$ 1,500.00	$ 1,450.50
World Wide Technology Program Management for Managed Services			
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 125,000 - 249,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.21
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 250,000 - 374,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.11
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 375,000 - 499,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.01
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 500,000+ Endpoints Per Endpoint	$ 25,000.00	$ 3.91
World Wide Technology Managed Services			
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 19.71
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 250,000 - 374,999 Endpoints	$ 25,000.00	$ 19.12

PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 375,000 - 499,999 Endpoints	$ 25,000.00	$ 18.45
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 500,000+ Endpoints	$ 25,000.00	$ 17.53
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Patch & Deploy Module - 125,000 - 249,999 Endpoints - Per Endpoint	$ 25,000.00	$ 5.33
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Patch & Deploy Module - 250,000 - 374,999 Endpoints - Per Endpoint	$ 25,000.00	$ 5.17
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Patch & Deploy Module - 375,000 - 499,999 Endpoints - Per Endpoint	$ 25,000.00	$ 4.97
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Patch & Deploy Module - 500,000 Endpoints - Per Endpoint	$ 25,000.00	$ 4.72

Bundle 3: Tanium Modules: Core Suite, Threat Response, Impact, Enforce, Comply, and SBOM

Implementation and Licensing Tanium Modules: Core, Threat Response, Impact, Enforce, Comply, and SBOM Initial Term Pricing (Years 1-3)		
Item No.	**Description**	**Rate Per Device/Endpoint**
1	**<u>Initial Software Year</u>** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$33.29 - 125,000 to 249,999 $31.81 - 250,000 to 374,999 $30.40 - 375,000 to 499,999 $29.05 - 500,000+
2	**<u>Subsequent Software Year</u>** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$28.88 - 125,000 to 249,999 $27.44 - 250,000 to 374,999 $26.07 - 375,000 to 499,999 $24.76 - 500,000+

Implementation and Licensing Tanium Modules: Core, Threat Response, Impact, Enforce, Comply, and SBOM Renewal Term Pricing (Years 4-6) (Optional)		
Item No.	**Description**	**Rate Per Device/Endpoint**
1	**<u>Renewal Software Year (~15% higher than Year 1)</u>** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$38.28 - 125,000 to 249,999 $36.58 - 250,000 to 374,999 $34.95 - 375,000 to 499,999 $33.41 - 500,000+
2	**<u>Subsequent Software Year (5% increase each year)</u>** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$33.22 - 125,000 to 249,999 $31.56 - 250,000 to 374,999 $29.98 - 375,000 to 499,999 $28.48 - 500,000+

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
Tanium Waterfall Software SKUs			
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 26.75	$ 9.87
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 26.75	$ 9.37
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 26.75	$ 8.90
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Endpoints	$ 26.75	$ 8.46
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 21.00	$ 7.75
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 21.00	$ 7.36
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 21.00	$ 6.99
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 21.00	$ 6.64
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 5.50	$ 2.02
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 5.50	$ 1.92
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 5.50	$ 1.83
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 5.50	$ 1.73
TAN-ENFORCE-TAAS	Provision Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 3.00	$ 2.67

TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 7.25	$ 2.54
TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 7.25	$ 2.41
TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 7.25	$ 2.29
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 10.00	$ 4.10
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 10.00	$ 3.90
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 10.00	$ 3.70
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 10.00	$ 3.52
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 3.00	$ 1.23
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 3.00	$ 1.17
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 3.00	$ 1.11
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 3.00	$ 1.11
Tanium Training SKUs			
TAN-TRN-VIRTUAL-E	Essentials Virtual 1 yr	$ 16,950.00	$ -
WWT Implementation SKUs			
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 5.65
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 250,000 - 374,999 Endpoints	$ 25,000.00	$ 5.55
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 375,000 - 499,999 Endpoints	$ 25,000.00	$ 5.45
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 500,000+ Endpoints	$ 25,000.00	$ 5.35

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
Tanium Waterfall Software SKUs			
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 26.75	$ 10.85
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 26.75	$ 10.31
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 26.75	$ 9.80
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Endpoints	$ 26.75	$ 9.30
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 21.00	$ 8.52
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 21.00	$ 8.10
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 21.00	$ 7.69
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 21.00	$ 7.31
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 5.50	$ 2.22
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 5.50	$ 2.11
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 5.50	$ 2.01
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 5.50	$ 1.91
TAN-ENFORCE-TAAS	Provision Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 7.25	$ 3.24

TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 7.25	$ 3.08
TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 7.25	$ 2.93
TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 7.25	$ 2.78
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 10.00	$ 4.10
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 10.00	$ 3.90
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 10.00	$ 3.70
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 10.00	$ 3.52
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 3.00	$ 1.23
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 3.00	$ 1.17
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 3.00	$ 1.11
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 3.00	$ 1.11
Tanium Training SKUs			
TAN-TRN-VIRTUAL-E	Essentials Virtual 1 yr	$ 16,950.00	$ -

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
	Tanium Direct Connect/ScreenMeet		
SS-RMT	Remote Screen Share - 1 required per Customer Entity Administrator to facilitate RFQ Requirement in Section 6.1.16	$ 1,500.00	$ 1,450.50
	World Wide Technology Program Management for Managed Services		
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 125,000 - 249,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.21
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 250,000 - 374,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.11
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 375,000 - 499,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.01
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 500,000+ Endpoints Per Endpoint	$ 25,000.00	$ 3.91
	World Wide Technology Managed Services		
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 19.71
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 250,000 - 374,999 Endpoints	$ 25,000.00	$ 19.12
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 375,000 - 499,999 Endpoints	$ 25,000.00	$ 18.45
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 500,000+ Endpoints	$ 25,000.00	$ 17.53
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Enforce Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 4.00
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Enforce Module - 250,000 - 374,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.88
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Enforce Module - 375,000 - 499,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.72

PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Enforce Module - 500,000 Endpoints - Per Endpoint	$ 25,000.00	$ 3.53
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Comply Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 4.00
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Comply Module - 250,000 - 374,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.88
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Comply Module - 375,000 - 499,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.72
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Comply Module - 500,000 Endpoints - Per Endpoint	$ 25,000.00	$ 3.53
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium SBOM Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 3.33
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium SBOM Module - 250,000 - 374,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.23
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium SBOM Module - 375,000 - 499,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.20
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium SBOM Module - 500,000 Endpoints - Per Endpoint	$ 25,000.00	$ 3.04

Bundle 4: Tanium Modules: Core Suite, Threat Response, Impact, Enforce, Comply, SBOM, Reveal, Integrity Monitor, and Certificate Manager

Implementation and Licensing Tanium Modules: Core, Threat Response, Impact, Enforce, Comply, SBOM, Reveal, Integrity Monitor and Certificate Manager Initial Term Pricing (Years 1-3)		
Item No.	**Description**	**Rate Per Device/Endpoint**
1	**Initial Software Year** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$40.51 - 125,000 to 249,999 $38.66 - 250,000 to 374,999 $36.91 - 375,000 to 499,999 $35.23 - 500,000+
2	**Subsequent Software Year** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$36.42 - 125,000 to 249,999 $34.60 - 250,000 to 374,999 $32.87 - 375,000 to 499,999 $31.23 - 500,000+

Implementation and Licensing Tanium Modules: Core, Threat Response, Impact, Enforce, Comply, SBOM, Reveal, Integrity Monitor and Certificate Manager Renewal Term Pricing (Years 4-6) (Optional)		
Item No.	**Description**	**Rate Per Device/Endpoint**
1	**Renewal Software Year (~15% higher than Year 1)** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$46.58 - 125,000 to 249,999 $44.46 - 250,000 to 374,999 $42.44 - 375,000 to 499,999 $40.52 - 500,000+
2	**Subsequent Software Year (5% increase each year)** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$41.89 - 125,000 to 249,999 $39.79 - 250,000 to 374,999 $37.80 - 375,000 to 499,999 $35.91 - 500,000+

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
Tanium Waterfall Software SKUs			
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 26.75	$ 9.87
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 26.75	$ 9.37
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 26.75	$ 8.90
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Endpoints	$ 26.75	$ 8.46
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 21.00	$ 7.75
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 21.00	$ 7.36
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 21.00	$ 6.99
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 21.00	$ 6.64
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 5.50	$ 2.02
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 5.50	$ 1.92
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 5.50	$ 1.83
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 5.50	$ 1.73
TAN-ENFORCE-TAAS	Provision Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 3.00	$ 2.67

TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 7.25	$ 2.54
TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 7.25	$ 2.41
TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 7.25	$ 2.29
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 10.00	$ 4.10
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 10.00	$ 3.90
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 10.00	$ 3.70
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 10.00	$ 3.52
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 3.00	$ 1.23
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 3.00	$ 1.17
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 3.00	$ 1.11
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 3.00	$ 1.05
TAN-REVEAL-TAAS	Reveal Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 7.75	$ 2.86
TAN-REVEAL-TAAS	Reveal Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 7.75	$ 2.72
TAN-REVEAL-TAAS	Reveal Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 7.75	$ 2.58
TAN-REVEAL-TAAS	Reveal Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 7.75	$ 2.45

TAN-IM-TAAS	Integrity Monitor Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 8.00	$ 2.95
TAN-IM-TAAS	Integrity Monitor Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 8.00	$ 2.80
TAN-IM-TAAS	Integrity Monitor Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 8.00	$ 2.66
TAN-IM-TAAS	Integrity Monitor Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 8.00	$ 2.52
TAN-CERTMAN-TAAS	Certificate Manager Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 3.00	$ 1.11
TAN-CERTMAN-TAAS	Certificate Manager Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 8.00	$ 1.06
TAN-CERTMAN-TAAS	Certificate Manager Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 8.00	$ 1.00
TAN-CERTMAN-TAAS	Certificate Manager Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 8.00	$ 0.95
Tanium Training SKUs			
TAN-TRN-VIRTUAL-E	Essentials Virtual 1 yr	$ 16,950.00	$ -
WWT Implementation SKUs			
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 5.65
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 250,000 - 374,999 Endpoints	$ 25,000.00	$ 5.55
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 375,000 - 499,999 Endpoints	$ 25,000.00	$ 5.45
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 500,000+ Endpoints	$ 25,000.00	$ 5.35

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
Tanium Waterfall Software SKUs			
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 26.75	$ 10.85
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 26.75	$ 10.31
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 26.75	$ 9.80
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Endpoints	$ 26.75	$ 9.30
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 21.00	$ 8.52
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 21.00	$ 8.10
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 21.00	$ 7.69
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 21.00	$ 7.31
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 5.50	$ 2.22
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 5.50	$ 2.11
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 5.50	$ 2.01
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 5.50	$ 1.91
TAN-ENFORCE-TAAS	Provision Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 7.25	$ 3.24

TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 7.25	$ 3.08
TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 7.25	$ 2.93
TAN-ENFORCE-TAAS	Enforce Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 7.25	$ 2.78
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 10.00	$ 4.10
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 10.00	$ 3.90
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 10.00	$ 3.70
TAN-COMPPLUS-TAAS	Comply Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 10.00	$ 3.52
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 3.00	$ 1.23
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 3.00	$ 1.17
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 3.00	$ 1.11
TAN-SBOM-TAAS	SBOM Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 3.00	$ 1.05
TAN-REVEAL-TAAS	Reveal Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 7.75	$ 2.99
TAN-REVEAL-TAAS	Reveal Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 7.75	$ 2.84
TAN-REVEAL-TAAS	Reveal Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 7.75	$ 2.70
TAN-REVEAL-TAAS	Reveal Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 7.75	$ 2.56

TAN-IM-TAAS	Integrity Monitor Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 8.00	$ 3.08
TAN-IM-TAAS	Integrity Monitor Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 8.00	$ 2.92
TAN-IM-TAAS	Integrity Monitor Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 8.00	$ 2.78
TAN-IM-TAAS	Integrity Monitor Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 8.00	$ 2.64
TAN-CERTMAN-TAAS	Certificate Manager Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 3.00	$ 1.16
TAN-CERTMAN-TAAS	Certificate Manager Module based on Per Endpoint - Minimum Purchase of 250,000 Endpoints is Required for this Purchase - 250,000-374,999 Users	$ 8.00	$ 1.10
TAN-CERTMAN-TAAS	Certificate Manager Module based on Per Endpoint - Minimum Purchase of 375,000 Endpoints is Required for this Purchase - 375,000-499,999 Users	$ 8.00	$ 1.05
TAN-CERTMAN-TAAS	Certificate Manager Module based on Per Endpoint - Minimum Purchase of 500,000 Endpoints is Required for this Purchase - 500,000+ Users	$ 8.00	$ 1.00
Tanium Training SKUs			
TAN-TRN-VIRTUAL-E	Essentials Virtual 1 yr	$ 16,950.00	$ -

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
Tanium Direct Connect/ScreenMeet			
SS-RMT	Remote Screen Share - 1 required per Customer Entity Administrator to facilitate RFQ Requirement in Section 6.1.16	$ 1,500.00	$ 1,450.50
World Wide Technology Program Management for Managed Services			
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 125,000 - 249,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.21
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 250,000 - 374,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.11

PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 375,000 - 499,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.01
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 500,000+ Endpoints Per Endpoint	$ 25,000.00	$ 3.91
World Wide Technology Managed Services			
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 19.71
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 250,000 - 374,999 Endpoints	$ 25,000.00	$ 19.12
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 375,000 - 499,999 Endpoints	$ 25,000.00	$ 18.45
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 500,000+ Endpoints	$ 25,000.00	$ 17.53
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Enforce Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 4.00
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Enforce Module - 250,000 - 374,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.88
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Enforce Module - 375,000 - 499,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.72
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Enforce Module - 500,000 Endpoints - Per Endpoint	$ 25,000.00	$ 3.53
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Comply Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 4.00
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Comply Module - 250,000 - 374,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.88
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Comply Module - 375,000 - 499,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.72

PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Comply Module - 500,000 Endpoints - Per Endpoint	$ 25,000.00	$ 3.53
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium SBOM Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 3.33
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium SBOM Module - 250,000 - 374,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.23
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium SBOM Module - 375,000 - 499,999 Endpoints - Per Endpoint	$ 25,000.00	$ 3.20
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium SBOM Module - 500,000 Endpoints - Per Endpoint	$ 25,000.00	$ 3.04
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Reveal Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 5.33
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Reveal Module - 250,000 - 374,999 Endpoints - Per Endpoint	$ 25,000.00	$ 5.17
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Reveal Module - 375,000 - 499,999 Endpoints - Per Endpoint	$ 25,000.00	$ 4.96
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Reveal Module - 500,000 Endpoints - Per Endpoint	$ 25,000.00	$ 4.71
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Integrity Monitor Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 6.67
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Integrity Monitor - 250,000 - 374,999 Endpoints - Per Endpoint	$ 25,000.00	$ 6.47
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Integrity Monitor - 375,000 - 499,999 Endpoints - Per Endpoint	$ 25,000.00	$ 6.21
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Integrity Monitor - 500,000 Endpoints - Per Endpoint	$ 25,000.00	$ 5.90

PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Certificate Manager Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 1.33
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Certificate Manager - 250,000 - 374,999 Endpoints - Per Endpoint	$ 25,000.00	$ 1.29
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Certificate Manager - 375,000 - 499,999 Endpoints - Per Endpoint	$ 25,000.00	$ 1.24
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Certificate Manager - 500,000 Endpoints - Per Endpoint	$ 25,000.00	$ 1.18

Pricing for Customer Entity On Their Own (Separate Tanium Cloud Instance)
Non-CSOC Entity

The following option if for a Customer Entity that will be outside the Florida CSOC. The Customer Entity will be deployed into their own cloud instance separate from the CSOC. A minimum of 125,000 devices will need to be purchased to be eligible for the pricing below. Customer's that have a license count that is less that 125,000, please see the following pricing scenario.

The Customer Entity will need to purchase on their training classes as well. Training will need to be purchased at $8,647.96 for the initial person, and then $306.12 for each additional person. All names must be given at the start of the training subscription to receive the add-on price.

Implementation and Licensing
Tanium Modules: Core, Threat Response, and Impact
Initial Term Pricing (Years 1-3)

Item No.	Description	Rate Per Device/Endpoint
1	**Initial Software Year** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$ 57.14
2	**Subsequent Software Year** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$ 51.49

Implementation and Licensing Tanium Modules: Core, Threat Response, and Impact Renewal Term Pricing (Years 4-6) (Optional)		
Item No.	**Description**	**Rate Per Device/Endpoint**
1	**<u>Renewal Software Year (~15% higher than Year 1)</u>** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$ 65.71
2	**<u>Subsequent Software Year (5% increase each year)</u>** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$ 59.22

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
Tanium Waterfall Software SKUs			
TAN-CORE-TAAS	Tanium Core Platform - Tanium Cloud	$ 26.75	$ 25.87
TAN-TR-TAAS	Tanium Threat Response - Tanium Cloud	$ 21.00	$ 20.31
TAN-IMPACT-TAAS	Tanium Impact - Tanium Cloud	$ 5.50	$ 5.32
WWT Implementation SKUs			
PS-SUPP-1	World Wide Technology - Implementation Services for 1 Year - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 5.65

Item No. 2 – ACS Pricing Breakdown
(without implementation)

ACS SKU Number	ACS SKU Description	Market Price	ACS Price
Tanium Waterfall Software SKUs			
TAN-CORE-TAAS	Core Platform based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 26.75	$ 10.85
TAN-TR-TAAS	Threat Response Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 21.00	$ 8.52
TAN-IMPACT-TAAS	Impact Module based on Per Endpoint - Minimum Purchase of 125,000 Endpoints is Required for this Purchase - 125,000-249,999 Users	$ 5.50	$ 2.22

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
Tanium Optional Modules			
TAN-PTCH2-TAAS	Tanium Patch 2 - Tanium Cloud	$ 8.00	$ 7.74
TAN-DEPLOY-TAAS	Tanium Deploy - Tanium Cloud	$ 8.00	$ 7.74
TAN-ENFORCE-TAAS	Tanium Enforce - Tanium Cloud	$ 3.00	$ 2.90
TAN-COMPPLUS-TAAS	Tanium Comply Plus - Tanium Cloud	$ 10.00	$ 9.67
TAN-SBOM-TAAS	Tanium SBOM Module - Tanium Cloud	$ 3.00	$ 2.90
TAN-REVEAL-TAAS	Tanium Reveal - Tanium Cloud	$ 7.75	$ 7.49
TAN-IM-TAAS	Tanium Integrity Monitor - Tanium Cloud	$ 8.00	$ 7.74
TAN-CERTMAN-TAAS	Tanium Certificate Manager - Tanium Cloud	$ 3.00	$ 2.90
Tanium Direct Connect/ScreenMeet			
SS-RMT	Remote Screen Share - 1 required per Customer Entity Administrator to facilitate RFQ Requirement in Section 6.1.16	$ 1,500.00	$ 1,450.50
Tanium Training SKUs			
TAN-TRN-VIRTUAL-E	Essentials Virtual 1 yr	$ 16,950.00	$ 8,647.96

TAN-TRN-VIRTUAL-E-AS	Tanium Essentials - Virtual - Additional Student. 1 Year Expiration	$ 600.00	$ 306.12
World Wide Technology Program Management for Managed Services			
PS-SUPP-1	World Wide Technology - Program Management for Managed Services for 1 Year - 125,000 - 249,999 Endpoints Per Endpoint	$ 25,000.00	$ 4.21
World Wide Technology Managed Services			
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Core Platform, Threat Response Module, & Impact Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 19.71
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Enforce Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 4.00
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Patch & Deploy Modules - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 5.33
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Comply Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 4.00
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium SBOM Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 3.33
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Reveal Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 5.33
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Integrity Monitor Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 6.67
PS-SUPP-1	World Wide Technology - Managed Services for 1 Year - Tanium Certificate Manager Module - 125,000 - 249,999 Endpoints	$ 25,000.00	$ 1.33

MSSP Solution
Pricing for Customer Entity On Their Own (Separate Tanium Cloud Instance) - Non-CSOC Entity – under 1,000 Devices

The following option if for a Customer Entity that will be outside the Florida CSOC. The Customer Entity will be deployed into their own cloud instance separate from the CSOC with less than 1,000 devices. A minimum purchase of 1,000 devices is required to begin this service. The initial service can be split between multiple Customer Entities, however, a total of 1,000 of endpoints are required to begin. This will require purchasing the World Wide Technology Managed Security Service Provider (MSSP) solution. This includes, implementation, managed services, and the software modules found in Bundle 1.

ScreenMeet is required to meet the requirement of Section 6.1.16 of the RFQ Requirements. This is a per named user cost and not a per device cost and is only needed for each of the Customer Entity's number of administrators at a cost of $1,450 per named user. This price will need to be added to each purchase option to comply with the RFQ requirements.

The Customer Entity will need to purchase on their training classes as well. Training will need to be purchased at $8,647.96 for the initial person, and then $306.12 for each additional person. All names must be given at the start of the training subscription to receive the add-on price.

MSSP Solution: Includes: Implementation, Managed Service, and Licensing
Tanium Modules: Core, Threat Response, Impact, Enforce, Comply, SBOM, Reveal, Integrity Monitor and Certificate Manager
Initial Term Pricing (Years 1-3)

Item No.	Description	Rate Per Device/Endpoint
1	**Initial Software Year** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$ 193.11
2	**Subsequent Software Year** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$ 193.11

MSSP Solution: Includes: Implementation, Managed Service, and Licensing Tanium Modules: Core, Threat Response, Impact, Enforce, Comply, SBOM, Reveal, Integrity Monitor and Certificate Manager Renewal Term Pricing (Years 4-6) (Optional)		
Item No.	**Description**	**Rate Per Device/Endpoint**
1	**Renewal Software Year (~15% higher than Year 1)** One year of endpoint detection and response software Solution as described in the RFQ per device. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$ 222.08
2	**Subsequent Software Year (5% increase each year)** One year of endpoint-based asset discovery (agent) software Solution as described in the RFQ per device/endpoint. To include: • ongoing training • integration maintenance • support services	$ 233.18

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
World Wide Technology MSSP - Implementation, Licensing, and Managed Services Included			
PS-SUPP-1	Core Platform with the Threat Response, Impact, Enforce, Comply, SBOM, Reveal, Integrity Monitor and Certificate Manager Modules - based on Per Endpoint - Minimum Purchase of 1,000 Endpoints is Required for this Purchase	$ 25,000.00	$ 193.11

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
World Wide Technology MSSP - Licensing and Managed Services Included			
PS-SUPP-1	Core Platform with the Threat Response, Impact, Enforce, Comply, SBOM, Reveal, Integrity Monitor and Certificate Manager Modules - based on Per Endpoint - Minimum Purchase of 1,000 Endpoints is Required for this Purchase	$ 25,000.00	$ 193.11

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**
Tanium Direct Connect/ScreenMeet			
SS-RMT	Remote Screen Share - 1 required per Customer Entity Administrator to facilitate RFQ Requirement in Section 6.1.16	$ 1,500.00	$ 1,450.50
Tanium Training SKUs			
TAN-TRN-VIRTUAL-E	Essentials Virtual 1 yr	$ 16,950.00	$ 8,647.96
TAN-TRN-VIRTUAL-E-AS	Tanium Essentials - Virtual - Additional Student. 1 Year Expiration	$ 600.00	$ 306.12

WWT/Foresite's Security Operations Platform Essential Per Person

The below pricing is for the Foresite Security Operations Platform. The customer entity can add this SOP solution to monitor the Tanium Bundles above and listed in Section V. If Foresite is managing both the Tanium instance and the SOP for the customer entity, price will be reevaluated to be at a lower cost to the customer.

The following solution is for WWT/Foresite’s Security Operations Platform, Essentials version, utilizing Foresite’s ProVision.

Initial Term Pricing (Years 1-3)		
Item No.	Description	Rate Per User
1	**Initial Software Year** One year of security operations platform software Solution as described in the RFQ per user. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$ 68.21
2	**Subsequent Software Year** Initial Software Year One year of security operations platform software Solution as described in the RFQ per user. To include: • ongoing training • integration maintenance • support services	$ 68.21

Initial Term Pricing (Years 4-6)		
Item No.	Description	Rate Per User
1	**Renewal Software Year - ~15% Higher than Year 1** One year of security operations platform software Solution as described in the RFQ per user. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$ 78.44

2	**Subsequent Software Year - ~5% YoY Increase** Initial Software Year One year of security operations platform software Solution as described in the RFQ per user. To include: • ongoing training • integration maintenance • support services	$ 82.36

Item No. 1 - ACS Pricing Breakdown WWT/Foresite's Security Operations Platform Essential Per Person - SKU Breakdown			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
World Wide Technology Security Operations Platform - Pricing per Device Per Year			
PS-SUPP-1	ProVision Essential - Per User Pricing Standard offering - 24x7x365 Security Operation Center - Includes ingestion from the supported list (https://foresite.com/docs/supported-assets) - Assets are limited by size of the organization based on user count (tiering) - Incident Response Support - Free Monthly Training from Technical Account Manager	$ 25,000.00	$ 64.00
WWT Program Management Pricing per User Per Year			
PS-SUPP-1	WWT Program Management - Up to 10,0000 - Per User Pricing	$ 25,000.00	$ 4.21

Item No. 2 – ACS Pricing Breakdown (without implementation) WWT/Foresite's Security Operations Platform Essential Per Person - SKU Breakdown			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
World Wide Technology Security Operations Platform - Pricing per Device Per Year			
PS-SUPP-1	ProVision Essential - Per User Pricing Standard offering - 24x7x365 Security Operation Center - Includes ingestion from the supported list (https://foresite.com/docs/supported-assets) - Assets are limited by size of the organization based on user count (tiering) - Incident Response Support - Free Monthly Training from Technical Account Manager	$ 25,000.00	$ 64.00
WWT Program Management Pricing per User Per Year			
PS-SUPP-1	WWT Program Management - Up to 10,0000 - Per User Pricing	$ 25,000.00	$ 4.21

Item No. 3 – ACS Pricing Breakdown Optional Add-On SKUs			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
World Wide Technology Security Operations Platform - Pricing per Device Per Year			

PS-SUPP-1	Production Telemetry - Per TB	$ 25,000.00	$ 2,022.00
PS-SUPP-1	Patch Management - ProVision Patch Management Service (Workstation)	$ 25,000.00	$ 61.92
PS-SUPP-1	Patch Management - ProVision Patch Management Service (Server)	$ 25,000.00	$ 81.48
PS-SUPP-1	Additional Assets - Per Device Per Year	$ 25,000.00	$ 437.30
PS-SUPP-1	Managed Detection & Response (MDR) - ProVision Managed Detection & Response (MDR) (No License)	$ 25,000.00	$ 25.56
PS-SUPP-1	Managed Detection & Response (MDR) - ProVision Managed Detection & Response (MDR) + CrowdStrike MSSP Defend Bundle	$ 25,000.00	$ 60.69
PS-SUPP-1	Managed Detection & Response (MDR) - ProVision Managed Detection & Response (MDR) + CrowdStrike MSSP Advanced Defend Bundle	$ 25,000.00	$ 71.98
PS-SUPP-1	Automated Breach & Attack Simulation + Red Team Services - Automated Breach and Attack Simulation+ Red Team Services	$ 25,000.00	$ 13.33
PS-SUPP-1	Firewall Management - ProVision Firewall Management (Small: 2GB)	$ 25,000.00	$ 814.80
PS-SUPP-1	Firewall Management - ProVision Firewall Management (Standard: 20GB)	$ 25,000.00	$ 1,290.00
PS-SUPP-1	Firewall Management - ProVision Firewall Management (Enterprise: 40GB)	$ 25,000.00	$ 2,150.17

WWT/Foresite's Security Operations Platform Elite Per Person

The following solution is for WWT/Foresite's Security Operations Platform, Elite version, utilizing Foresite's ProVision.

Initial Term Pricing (Years 1-3)		
Item No.	**Description**	**Rate Per Device**
1	**Initial Software Year** One year of security operations platform software Solution as described in the RFQ per user. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$ 128.21
2	**Subsequent Software Year** Initial Software Year One year of security operations platform software Solution as described in the RFQ per user. To include: • ongoing training • integration maintenance • support services	$ 128.21

Optional Renewal Term Pricing (Years 4-6)		
Item No.	**Description**	**Rate Per Device**
1	**Renewal Software Year - ~15% Higher than Year 1** One year of security operations platform software Solution as described in the RFQ per user. To include: • implementation • initial training • initial Integration • integration maintenance • support services	$ 147.44
2	**Subsequent Software Year - ~5% YoY Increase** Initial Software Year One year of security operations platform software Solution as described in the RFQ per user. To include: • ongoing training • integration maintenance • support services	$ 154.81

Item No. 1 - ACS Pricing Breakdown WWT/Foresite's Security Operations Platform Elite Per Person - SKU Breakdown			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
World Wide Technology Security Operations Platform - Pricing per Device Per Year			
PS-SUPP-1	ProVision Elite - Per User Pricing - 24x7x365 Security Operation Center - Powered by Google Chronicle - Includes ingestion from the supported list (https://foresite.com/docs/supported-assets) - SOAR, MITR alignment, AI/Machine Learning, Threat Hunting, Incident Response Support, Unlimited corporate telemetry, Free Monthly Training from Technical Account Manager	$ 25,000.00	$ 124.00
WWT Program Management Pricing per User Per Year			
PS-SUPP-1	WWT Program Management - Up to 10,0000 - Per User Pricing	$ 25,000.00	$ 4.21

Item No. 2 – ACS Pricing Breakdown (without implementation) WWT/Foresite's Security Operations Platform Elite Per Person - SKU Breakdown			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
World Wide Technology Security Operations Platform - Pricing per Device Per Year			
PS-SUPP-1	ProVision Elite - Per User Pricing - 24x7x365 Security Operation Center - Powered by Google Chronicle - Includes ingestion from the supported list (https://foresite.com/docs/supported-assets) - SOAR, MITR alignment, AI/Machine Learning, Threat Hunting, Incident Response Support, Unlimited corporate telemetry, Free Monthly Training from Technical Account Manager	$ 25,000.00	$ 124.00
WWT Program Management Pricing per User Per Year			
PS-SUPP-1	WWT Program Management - Up to 10,0000 - Per User Pricing	$ 25,000.00	$ 4.11

Item No. 3 – ACS Pricing Breakdown Optional Add-On SKUs			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
World Wide Technology Security Operations Platform - Pricing per Device Per Year			
PS-SUPP-1	Production Telemetry - Per TB	$ 25,000.00	$ 2,022.00
PS-SUPP-1	Patch Management - ProVision Patch Management Service (Workstation)	$ 25,000.00	$ 61.92
PS-SUPP-1	Patch Management - ProVision Patch Management Service (Server)	$ 25,000.00	$ 81.48
PS-SUPP-1	Additional Assets - Per Device Per Year	$ 25,000.00	$ 437.30
PS-SUPP-1	Managed Detection & Response (MDR) - ProVision Managed Detection & Response (MDR) (No License)	$ 25,000.00	$ 25.56

PS-SUPP-1	Managed Detection & Response (MDR) - ProVision Managed Detection & Response (MDR) + CrowdStrike MSSP Defend Bundle	$ 25,000.00	$ 60.69
PS-SUPP-1	Managed Detection & Response (MDR) - ProVision Managed Detection & Response (MDR) + CrowdStrike MSSP Advanced Defend Bundle	$ 25,000.00	$ 71.98
PS-SUPP-1	Automated Breach & Attack Simulation + Red Team Services - Automated Breach and Attack Simulation+ Red Team Services	$ 25,000.00	$ 13.33
PS-SUPP-1	Firewall Management - ProVision Firewall Management (Small: 2GB)	$ 25,000.00	$ 814.80
PS-SUPP-1	Firewall Management - ProVision Firewall Management (Standard: 20GB)	$ 25,000.00	$ 1,290.00
PS-SUPP-1	Firewall Management - ProVision Firewall Management (Enterprise: 40GB)	$ 25,000.00	$ 2,150.17

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 included in the optional bundles above.

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 included in the bundle options above.

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

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

Not provided in this submission.

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.

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.

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.

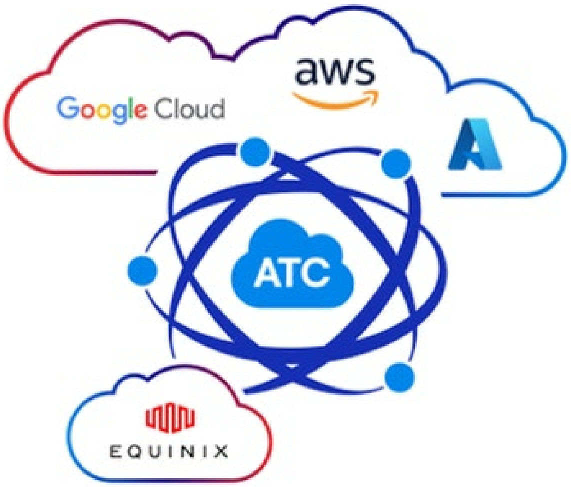


Figure 1
The ATC infrastructure facilitates fast proofs of concept for current and future use cases

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

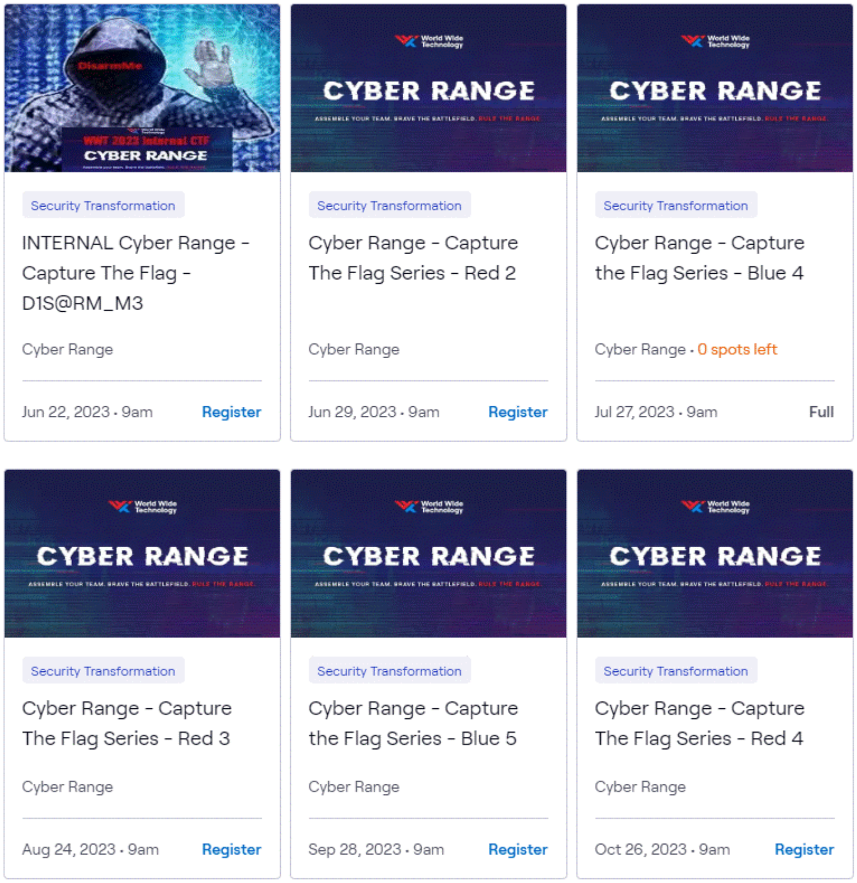
WWT Cyber Range

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 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:



Security Transformation
INTERNAL Cyber Range - Capture The Flag - D1S@RM_M3
Cyber Range
Jun 22, 2023 · 9am Register

Security Transformation
Cyber Range - Capture The Flag Series - Red 2
Cyber Range
Jun 29, 2023 · 9am Register

Security Transformation
Cyber Range - Capture the Flag Series - Blue 4
Cyber Range · 0 spots left
Jul 27, 2023 · 9am Full

Security Transformation
Cyber Range - Capture The Flag Series - Red 3
Cyber Range
Aug 24, 2023 · 9am Register

Security Transformation
Cyber Range - Capture the Flag Series - Blue 5
Cyber Range
Sep 28, 2023 · 9am Register

Security Transformation
Cyber Range - Capture The Flag Series - Red 4
Cyber Range
Oct 26, 2023 · 9am Register

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:

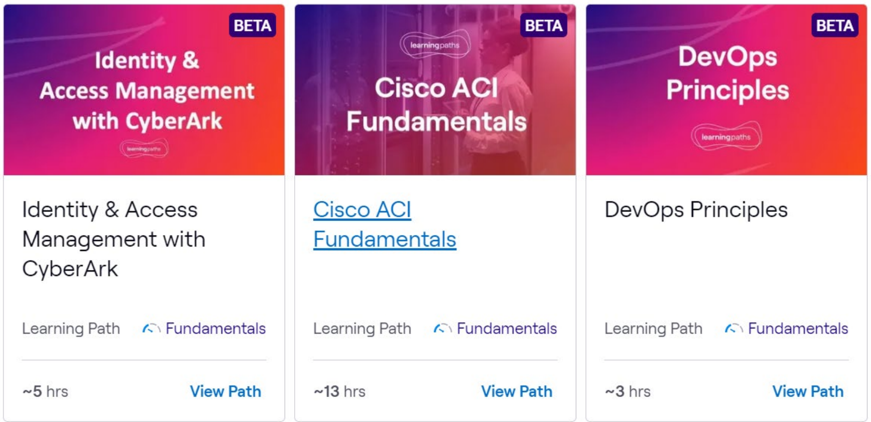
- Get hands-on, on-demand experience
- Capture real-world insights and research
- Leverage practical and actionable guidance
- Compare, contrast and validate multi-vendor solutions
- Think creatively about strategy
- Tap into our industry-leading expertise and unparalleled training

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.



Identity & Access Management with CyberArk

Learning Path | Fundamentals

~5 hrs | View Path

Cisco ACI Fundamentals

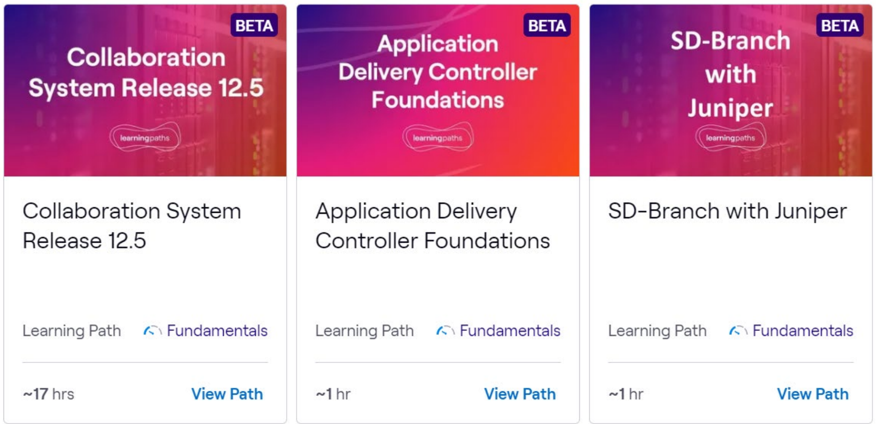
Learning Path | Fundamentals

~13 hrs | View Path

DevOps Principles

Learning Path | Fundamentals

~3 hrs | View Path


BETA
Collaboration System Release 12.5
learningpaths
BETA
Application Delivery Controller Foundations
learningpaths
BETA
SD-Branch with Juniper
learningpaths

Collaboration System Release 12.5

Learning Path | Fundamentals

~17 hrs | View Path

Application Delivery Controller Foundations

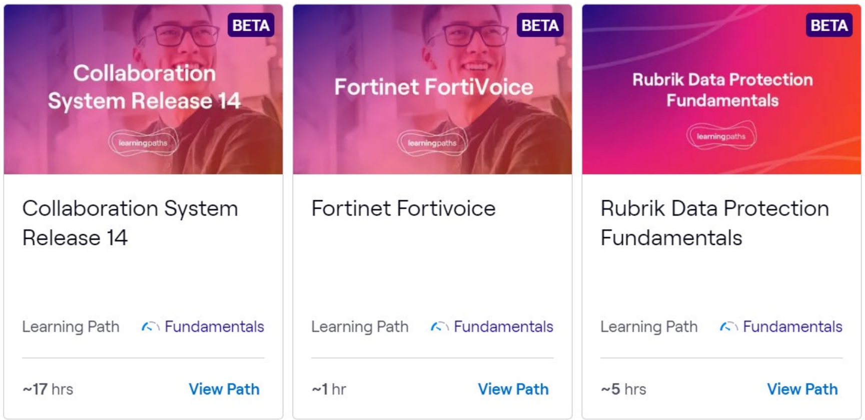
Learning Path | Fundamentals

~1 hr | View Path

SD-Branch with Juniper

Learning Path | Fundamentals

~1 hr | View Path



Collaboration System Release 14

Learning Path | Fundamentals

~17 hrs | View Path

Fortinet Fortivoice

Learning Path | Fundamentals

~1 hr | View Path

Rubrik Data Protection Fundamentals

Learning Path | Fundamentals

~5 hrs | View Path

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?”

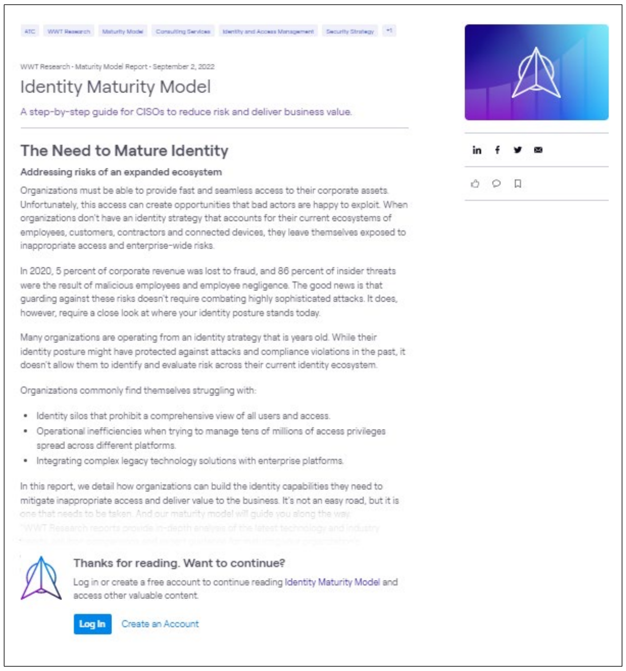
Our goal is to focus on the Department’s particular security needs and create a plan for a successful, optimized security transformation strategy.   Sessions are scheduled for 50 minutes total, with 20 minutes for thought leadership exploration and 30-minutes for interactive dialogue and discussion.

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.



WWT Research - Maturity Model Report - September 2, 2022

Identity Maturity Model

A step-by-step guide for CISOs to reduce risk and deliver business value.

The Need to Mature Identity

Addressing risks of an expanded ecosystem

Organizations must be able to provide fast and seamless access to their corporate assets. Unfortunately, this access can create opportunities that bad actors are happy to exploit. When organizations don't have an identity strategy that accounts for their current ecosystems of employees, customers, contractors and connected devices, they leave themselves exposed to inappropriate access and enterprise-wide risks.

In 2020, 5 percent of corporate revenue was lost to fraud, and 86 percent of insider threats were the result of malicious employees and employee negligence. The good news is that guarding against these risks doesn't require combating highly sophisticated attacks. It does, however, require a close look at where your identity posture stands today.

Many organizations are operating from an identity strategy that is years old. While their identity posture might have protected against attacks and compliance violations in the past, it doesn't allow them to identify and evaluate risk across their current identity ecosystem.

Organizations commonly find themselves struggling with:

- Identity silos that prohibit a comprehensive view of all users and access.
- Operational inefficiencies when trying to manage tens of millions of access privileges spread across different platforms.
- Integrating complex legacy technology solutions with enterprise platforms.

In this report, we detail how organizations can build the identity capabilities they need to mitigate inappropriate access and deliver value to the business. It's not an easy road, but it is one that needs to be taken. And our maturity model will guide you along the way.
*WWT Research reports provide in-depth analysis of the latest technology and industry trends, solution comparisons and expert guidance for maturing your organization's

Thanks for reading. Want to continue?

Log in or create a free account to continue reading Identity Maturity Model and access other valuable content.

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

WWT Presents
RESEARCH
Jill Cochrane and Matt Berry on Observability and Visibility

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

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

Signature

43-1912895

FEIN

Gregory Brush

Signatory Printed Name

May 12, 2023

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:	Perry Bright	Carol Harting
Title:	Client Manager	Business Development Mgr
Address (Line 1):	1 World Wide Way	1 World Wide Way
Address (Line 2):	N/A	N/A
City, State, Zip Code	St. Louis, MO 63146	St. Louis, MO 63146
Telephone (Office):	N/A	314-995-6103
Telephone (Mobile):	850-803-0076	636-751-8399
Email:	perry.bright@wwt.com	carol.harting@wwt.com

Department of
MANAGEMENT
SERVICES
▶ We Serve Those Who Serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950

Ron DeSantis, Governor
Pedro Allende, Secretary

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

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-22/23-157, Security Operations Platform Solution ("Solution");

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

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

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

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

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

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

(f) State: The State of Florida.

2. **Term and Termination.** This Agreement is effective upon signature by both Parties. This Agreement may be terminated by the Department when determined to be in the best interest of the State of Florida by providing Recipient with advance written notice.

3. **Intended Third Party Beneficiary.** Customers receiving services under the Solution are intended third party beneficiaries of this Agreement, entitled to enforce any rights hereunder for their benefit.

4. **Confidential Information Use.** Use of the Confidential Information shall be limited to the provisions set forth herein and to the extent necessary to provide the services and/or commodities. The Department retains full rights and title to all Confidential Information provided by it, and any information derived therefrom. Recipient has no ownership rights to the Confidential Information provided under this Agreement, or any information derived therefrom.

5. **Recipient Obligations.** Recipient shall: 1) maintain the confidentiality of all the Confidential Information pursuant to this Agreement, as required herein, 2) comply with all federal and State laws and regulations related to information privacy and security, and 3) ensure that any Affiliates comply with the preceding two requirements as to any Confidential Information shared with or otherwise Accessed by the Affiliate. Recipient shall take all measures necessary to protect against improper Access to and/or disclosure or theft of the Confidential Information and will ensure only those individuals performing services contemplated in this Agreement will be permitted to Access the Confidential Information. Recipient shall perform the following measures to preserve the privacy, security, confidentiality, integrity, and accessibility of the Confidential Information which includes, but is not limited to:

   (a) Using the Confidential Information only to provide services and/or commodities as contemplated in this Agreement and not otherwise using the Confidential Information for Recipient's own benefit or the benefit of others, or in violation of any applicable laws or regulations;

   (b) Not creating derivative works based upon the Confidential Information, copying the Confidential Information, or publishing or disclosing the Confidential Information to any individual or entity except in accordance with this Agreement;

   (c) Implementing and maintaining protective administrative, technical, and organizational security measures appropriate to the nature of the Confidential Information to safeguard against unauthorized Access, disclosure, or theft of the Confidential Information;

   (d) Maintaining the confidentiality of the Confidential Information under this Agreement in accordance with Department policies and procedures and applicable State and federal laws and regulations;

(e) Storing and safeguarding the Confidential Information in a physically and electronically secure location where Access is limited to authorized persons;

(f) Maintaining an up-to-date list of individuals who are authorized to Access the Confidential Information;

(g) Instructing and requiring all individuals authorized to Access the Confidential Information to adhere to the confidentiality requirements set forth in this Agreement prior to being granted Access to the Confidential Information;

(h) Not allowing, through action or inaction, any Confidential Information to be sent by any medium, transmitted, or to be Accessed outside of the United States. For the purposes of this restriction, “Access” does not include remote support sessions for devices that might contain the Confidential Information; however, during the remote support session the Department requires Recipient to escort the remote support access and maintain visibility of the actions taken during the remote support access. Requests for remote access will be submitted to the Department’s Contract Manager. With approval, third parties may be granted time-limited terminal service access to information technology resources as necessary for fulfillment of related responsibilities. Remote connections are subject to detailed monitoring via two-way log reviews and the use of other tools; and

(i) Performing all actions necessary to assist with all tasks in furtherance of the Department’s efforts to comply with the obligations under Chapters 60FF and 60GG, Florida Administrative Code, as applicable.

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

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

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

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

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

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

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

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

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

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

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

FLORIDA DEPARTMENT OF MANAGEMENT SERVICES	**World Wide Technology, LLC**
By: ______________________________	By: Gregory Brush Digitally signed by Gregory Brush Date: 2023.05.12 14:03:41 -05'00'
Name: ______________________________	Name: Gregory Brush
Title: ______________________________	Title: Area Vice President, Public Sector
Date: ______________________________	Date: May 12, 2023

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:		

FORESITE CYBERSECURITY

Service Description

ProVision

Cybersecurity and Compliance Solutions

Last updated 17 February 2022

As used in this Service Description, "ProVision", "we" or "us" means Foresite Cybersecurity Inc., a Delaware corporation, if the billing address for your order is in the United States, and Foresite Unlimited Company, a company organized and existing under the laws of the United Kingdom, if the billing address for your order is outside the United States. All terms used but not defined in this Service Description are defined in the Terms of Service or other documents comprising the Agreement between you and us regarding your use of the Service Offering.

The Foresite Cybersecurity Privacy Notices describe how personal information may be collected, used, shared, or otherwise processed by Foresite Cybersecurity as a data controller. The Foresite Cybersecurity Privacy Notices are available at https://foresite.com/about/privacy-policy/.

CONTENT

ProVision Security-Operations & Compliance Platform Introduction

The ProVision Security-Operations & Compliance Platform is a cloud-native software solution that enables companies to custom-tailor SOC-as-Service solutions on demand for all their cybersecurity and compliance requirements.

ProVision delivers secure, agile outcomes from a single unified platform. The ProVision platform brings unprecedented observability, reporting, orchestration, automation, and response to all your cybersecurity functions.

ProVision solutions are delivered in a subscription model. Simply ❶Choose the modules that are right for your business. ❷Add licensing credits. ❸Go. -No onboarding fees. Add modules or upgrade at any time.

ProVision modules include:

ProVision Monitor	1. SIEM
ProVision Management	1. Critical Asset Management 2. Managed Detection & Response (MDR) 3. Patch Management
ProVision Assess & Assure	1. Security Testing 2. GRC Advisory 3. Foresite Integrated Risk Management (FIRM)

ProVision Overview

Definitions

Alert	A log received from the Device/Asset, parsed by VisionLink, and sent to ProVision.
Client or Customer	The company procuring the managed service.
Co-Management	Both the Client and Foresite have full access to the Device/Asset for any changes or updates.
Contract	The contractual agreement between the parties.
Device/Asset	A combination of hardware, software and licensing that is to be monitored/managed as part of the Service.

Event	An activity that has been identified by ProVision to represent a potential threat that warrants additional triage by the SOC analysts to determine the nature of the activity.
FIRM	Foresite's Integrated Risk Management Platform.
Incident	An activity positively identified and warrants immediate engagement of Client incident handling and response personnel.
Log	A record of activity written by a security device, network element, computing platform, etc. for such purposes as recording events, errors, status messages, or other operating details.
OBQ	Onboarding Questionnaire. A document or online tool to gather all the required information to set up the Service.
Onboarding	The activities and process to bring the Client into live Service.
PoC	Client point of contact for managed service.
ProVision/Portal	Foresite's next-generation cloud-based managed services platform.
Service	Types of service available including Monitoring, Management, Assessment and Assurance.
Service Level	Level of service dependent on the type of service.
SOC	Foresite global security operation centers with the primary SOC located in Overland Park, KS, and supporting operations centers located in East Hartford, CT and Farnborough, UK.
SOS	Scope of Services
Ticket	Comes in various forms such as, but not limited to: • ***Support Ticket*** – Used to log and progress Tickets of a support nature (e.g., creation of a new user). • ***Security Incident Ticket*** - An activity positively identified for further investigation that warrants follow up (e.g., Suspected Security Issue). • ***Change Request Ticket*** – Used for creating requests for workload to be implemented (e.g., updating a set of Rules). • ***Security Test*** – Used for security testing services such as Penetration Testing, Vulnerability Assessment.

VisionLink	Foresite's Client premise appliance responsible for log and security stream aggregation and processing as part of the cloud-based ProVision managed services platform.

Service Scope

Hours of Operation	Foresite's managed services are delivered through Foresite's Global Security Operations Centers (SOCs) which operate 24 hours per day, 7 days per week, and 365/6 days per year.
Language Support	All Services, Portal and communications are provided in English language only.
Remote Support	All activities are implemented and provided remotely. In the event of issues that require physical or local access, Client may at times be required for assistance to trouble shoot (e.g., system rebuild, power-cycle, reboot, or console access).
Telephone Support	Foresite SOC's are available 24x7 via a US and UK phone number. The call will always be directed to available security staff on shift. During busy periods, the call may go to voicemail and the team will aim to respond within 30 minutes.
Ticketing	Ticket types include but are not limited to the following: Security Incident, Support Ticket, Change Request, Project and Security Test. The assignee of a Ticket will always be a Foresite SOC representative and if the status of the Ticket is set to "Waiting for Customer', then the progress of the Ticket is the responsibility of the Client's designated POC(s). Tickets have 4 severity levels as below: • ***P1 Emergency*** – System down or potential security Incident that warrants urgent attention • ***P2 Critical*** – Significant impact that could lead to a security Incident or system outage if not addressed • ***P3 Warning*** – Moderate loss of functionality or security that should be addressed • ***P4 Informational*** – Supporting information and notification of behavior The SOC Analyst will work closely with the Client's designated POC(s) to progress and resolve the Ticket where appropriate. If Client does not respond to the Ticket in a timely manner, Foresite reserves the right to resolve or close the Ticket. Tickets can be updated/progressed within the ProVision Portal or via email by responding to the Ticket update email that will get sent to all those set as a

	'Follower' within the Ticket. 'Followers' can be automatically assigned for all Client Tickets or individually depending on the actual Ticket. 'Followers' are confirmed during Onboarding and can be adapted throughout the lifetime of the Contract.

Prerequisites & Client Responsibilities

The following requirements must be confirmed by the Client for the operation of the service:

Device/Asset	Suitable infrastructure to be included in the service.
Software License/Subscriptions	Any Device/Asset in the Service must have the appropriate full manufacturer's product license and subscriptions for the duration of the Service. Device/Assets of Software that are considered end-of-support by the manufacturer are not covered by the Service.
Hardware Support	All Devices/Assets must have the appropriate full manufacturer's maintenance for the duration of the Service.
Software limitations	Only the manufacturer's application(s) and operating system are to be installed and running on the Asset/Device.
Security Operation	All Devices/Assets that are brought into the Service must contain a valid rule base or configuration to protect the security of the Service. Foresite reserves the right to audit any such configurations and remedial work may be required to address any issues.
Connectivity	Client will ensure client-side access and connectivity to all Device/Assets as appropriate. Foresite is not responsible for resolving Client's Internet Service Provider (ISP) outages, or issues with Client's internal network or computing platform infrastructure.
Log Stream	Typically, syslog or via api but dependent on technology. It is the responsibility of the client to ensure the log stream is directed at VisionLink for Service operation.
Client Point of Contact (POC)	The Client is responsible for providing Foresite a primary point of contact (POC). The POC will provide access to knowledgeable technical staff, and/or third-party resources, to assist Foresite with any hands-on support or working with third-party vendors.
ProVision Manage	ProVision Monitor licensing is required for ProVision Management. VisionLink is required, which acts as a bastion host enabling the SOC Engineers to connect to customer infrastructure for on-prem equipment, is required.

	Foresite will require full read/write access to the Device/Asset under management.

ProVision Portal

The ProVision portal is your dashboard to all ProVision modules:

- View Dashboards for summary of Service
- Manage Devices/Assets and system inventory
- View and search Alert logs and Events
- Search, update and manage all types of Tickets
- Access the checklist used to manage the onboarding of a new customer
- Access the document repository and upload Client information
- Create and manage users
- View and update user profile and Client information
- Access and schedule Reports
- Create and manage templates for Assessment services
- Access appropriate Knowledge Base articles

Reporting

ProVision provides a multitude of preconfigured reports that are all available in the ProVision Portal. Reporting is very flexible, including custom and quick date ranges, Device/Asset or Account information, tabular, graphical, or numerical view in a variety of different formats including bar graphs, line graphs, heat maps, pie charts and more.

Reports can be downloaded as a .csv or .pdf and can also be emailed using the report scheduler.
Reporting includes but is not limited:

- Monthly Management Report (Overview of Service for the period)
- CISO Report (Overview of Service for CISO reporting)
- Estate (Users, Managed Assets/Devices, Compliance)
- Tickets (Management Report, Support Tickets, Security Tickets, Change Requests)
- Service specific reports for areas such as Patch Management, MDR and M365
- Authentication (Management Report, Summary Report, By User, By Device, By Disabled Accounts)
- Accounts (Created, Disabled, Deleted, Enabled, Locked, Password Activity)
- Security Analysis (Management Report, Events, Log Messages, Anti-Virus, Policy Changes)
- Traffic (Management Report, Dropped Traffic, By Source, By Destination, By Destination Port)

Additional Reports can be requested during onboarding and can be adapted throughout the lifetime of the Contract (subject to availability of data). With the aim of continuous improvement, Foresite reserves the right to add/remove/change the reporting within ProVision.

Onboarding

The Foresite Customer Success Management (CSM) team will work with Customer to manage ProVision onboarding. An in-app onboarding checklist will guide and track onboarding progress.

Onboarding times vary based on ProVision modules, project complexity, and customer commitment to provide access, resources, and technical requirements timely.

Service Level Agreement (SLA)

Availability of the ProVision Portal
Foresite's ProVision Portal is guaranteed available 99.99% of the time over a one-year period and measured annually.

SLA Failure Rebate:
At Client's request, Foresite will pay a rebate each year (following each 12 months of service) in the format of a service credit which can be used to purchase additional services or extend the service period if the SLA has not been met. Customer must log the request for a rebate as a Ticket in the ProVision Portal within 30 days of the proposed missed SLA. Total service credit Rebates cannot exceed 10% the total annual service charge.

Measure	Credit
Availability of the ProVision Portal	Half a day service credit for every whole hour the SLA is missed
Events (Response)	1 hour service credit for every P1 or P2 Event that misses the Response SLA
Tickets (Response)	1 hour service credit for every P1 or P2 Ticket that misses the Response SLA

Maintenance Window
With the unique ProVision infrastructure, it is very rare that maintenance windows are required that incur an interruption to ProVision or the Service. Should there be a requirement for a period to conduct any maintenance, Foresite reserves the right to communicate that maintenance window in advance through the notification system within ProVision.

Time-to-Respond
Measured from when the Event or Ticket is created to when it is first touched by a SOC Engineer.

	Priority	Time to Respond (TTR)
ProVision Monitoring Events	P1 Emergency	15 mins
	P2 Critical	30 mins
	P3 Warning	2 hours
	P4 Informational	n/a
ProVision Monitoring Tickets	P1 Critical Impact	1 hour
	P2 Significant Impact	4 hours
	P3 Normal/Minor	24 hours
	P4 Low/Information	48 hours
ProVision Management Events	P1 Emergency	1 hour
	P2 Critical	2 hours
	P3 Warning	8 hours
	P4 Informational	n/a
ProVision Management Tickets	P1 Critical Impact	TTR + 4 hours
	P2 Significant Impact	TTR + 8 hours
	P3 Normal/Minor	72 hours
	P4 Low/Information	7 days
Patch Management Tickets	P1 Critical Impact	1 hour
	P2 Significant Impact	4 hours
	P3 Normal/Minor	24 hours
	P4 Low/Information	48 hours

SLA Exceptions
The following exclusions are not included in the SLA calculation:

- Scheduled maintenance work required by Foresite
- Change management requirements affecting managed devices
- Circumstances beyond the reasonable control of Foresite
- Loss of connectivity due to Client connectivity issues or Client managed issues

Exclusions

The following (without limitation) are not included in the Service:

Site Visits (on-site Support)	Site visits are not included with the Service.
Services for Device/Assets not covered within the Service	

Remedial work	Issues caused by Client initiated Changes or failed Changes are not covered by the Service.

Foresite operates a Fair Use Policy for the number of Tickets and Change Requests used in the Service. There is no limit on the number of Security Incident and Support Tickets used but Foresite reserve the right to review the volume of Change Requests per Client if it is determined that the Change Requests are being improperly used.

ProVision Modules

ProVision modules are customizable per Client. Module licensing is required for each module to apply. Contact your Foresite reseller or Foresite Sales Director to add additional modules not covered in your current subscription.

ProVision Monitoring & Alerting (SIEM)

Foresite's Monitoring Service delivers real time cybersecurity monitoring providing visibility of cyber threats with actionable intelligence.

ProVision Monitoring includes:

Description	**Security Monitoring & Analysis**
ProVision Security Suite Portal	✓
Log Storage and Analysis	✓
Security Information Event Monitoring	✓
24x7x365 Analysis and Alerting	✓
Notification & Escalation	✓
Reporting	✓

Service Scope
Foresite will monitor and analyze the log stream from the devices/assets under service. The log source will vary dependent on technology but is typically via syslog or API.

Monitored services require VisionLink (Foresite log collector):

- VisionLink is Foresite's software, which typically is deployed on-premises, but may also be deployed in the cloud, or by Foresite in some circumstances to facilitate the collection of data connecting to ProVision.
- Foresite recommends deploying VisionLink on a customer provided virtual machine. Other options are available if necessary.

- Client shall make available log feeds to VisionLink for all monitored devices.

VisionLink Requirements:

- VM specifications depend on the number of Devices/Assets in the Service.
- Typically, Quad core, 500GB HDD and 4GB Memory
- Ubuntu 20.04 LTS (or later approved system)
- Client is responsible for ensuring the VM is always available for the service.

Alerting & Escalation

Log streams received by VisionLink are parsed, normalized, and sent to the ProVision threat engine for additional analysis. The business rules in the threat engine raise any suspicious logs or patterns of behavior to an Event. Event conditions that are deemed of interest or worthy of follow-up will be brought to the attention of the Client's designated PoC(s) by the creation of a ticket within ProVision.

Events are classified into 4 severities:

Emergency	Existence of conditions which indicate a potential security incident has occurred
Critical	Existence of conditions which indicate the presence of a potential security threat requiring attention
Warning	Potential Incidents that may have been averted but warrant investigation and confirmation
Informational	System and vendor information to bring additional context to higher priority Events

All progress of incidents will be tracked within ProVision tickets. The SOC may also call the Client depending on the severity of the Incident. Communication and escalation plan preferences are confirmed during onboarding and can be adapted throughout the lifetime of the Contract.

Log Retention

Foresite stores ProVision security stream data consisting of processed log information (Alerts) for a minimum period of 1 year unless otherwise specified in the Sales Order. 90 days of Alert logs are available and searchable online in the ProVision portal, with the additional 9 months being stored on offline storage. Additional storage requirements are available.

Additional Checks

Foresite can apply additional checks to a Device/Asset depending on requirement. These checks include ICMP (Ping), HTTP, HTTPS, & SSH. Any additional checks are confirmed during onboarding and can be adapted throughout the lifetime of the Contract.

ProVision Management

Reliable cybersecurity infrastructure management for firewall, NGAV, EDR, and more.

Get the most out of your security investment with:

- 24x7x365 access to skilled security professionals.
- Discover and remediate security gaps before they are a problem.
- We will help you with full incident analysis, remediation, change control, and system updates/upgrades.
- Completely managed or co-managed solutions.

PREREQUISITE
Requires ProVision Monitor

ProVision Management includes:

Description	**Security Monitoring & Analysis**
ProVision Security Suite Portal	✓
Log Storage and Analysis	✓
Security Information Event Monitoring	✓
24x7x365 Analysis and Alerting	✓
Notification & Escalation	✓
Reporting	✓
Incident Remediation	✓
Change Requests	✓
System Upgrades*	✓
System Configuration Backup**	Option

*System Upgrades are included for minor upgrades that can be performed remotely. If onsite work is recommended and required, this will be covered by an additional SOS.

**Backups of the Device/Asset are the responsibility of the Client. At Client request, Foresite will perform a manual configuration backup prior to implementing any Change Requests, subject to the technology allowing it.

Service Scope
Customer will choose a management program:

Co-Management	Customer has full read/write access to their infrastructure 1. Customer is required to document all changes they make via a change request ticket in ProVision. 2. Client can use a combination of Client implemented and Foresite implemented changes throughout the lifetime of the Service.

Full-Management	Client has read-only access to their infrastructure

Foresite will provide management services for the Device/Asset that includes policy updates, rule base changes and configuration changes as required for the operation of the service.

Managed Detection & Response

Protect your business with Managed Detection and Response (MDR) solutions. MDR Services provide better proactive defense than traditional managed security services alone. Foresite's MDR solutions enable a proactive and advanced approach to cybersecurity. Advanced detection of malicious activities through security threat hunting and monitoring significantly reduce days to response, and rapid incident analysis and response significantly lessons security breach costs.

Foresite will utilize an Endpoint Detection Response (EDR) technology (and other solutions based on delivery requirements if applicable) to investigate devices and network data within the organizations infrastructure to attempt to identify malicious and/or suspicious activity.

Using pro-active threat hunting techniques, the service is designed to uncover advanced threats potentially hiding within the organization.

Managed Detection and Response service options:

Description	**Standard**	**Advanced**
EDR Software	✓	✓
EDR Licenses	✓	✓
Threat Hunting Sessions per week	1	2
ProVision Platform	✓	✓
First Line Support/Management of the EDR platform	✓	✓
24x7x365 EDR monitoring	✓	✓
Policy Review	✓	✓
Custom Watchlist Alerting (*Carbon Black only*)	x	✓
Advance Reporting	x	✓
Proactive Response	x	✓

EDR licensing options:

Customer Provided	See Sales for current support technologies
Foresite Provided	**Standard:** VMWare CB Endpoint Standard **Advanced:** VMWare Enterprise Endpoint Detection and Response

Service Scope

Foresite's MDR service provides real-time security monitoring, analysis and identification of potential areas of compromise within the Client's estate. On top of managing the EDR platform, Foresite will proactively hunt the Client's estate for potentially hidden threats, known vulnerabilities, potential misconfigurations, and recommend policy tuning.

All Foresite activities are unobtrusive and conducted in the background with the customer only being alerted should a threat and/or vulnerability be discovered. Identified and potential threats will be logged as Security Incident Tickets and progressed/mitigated as per the section above on Ticketing.

Threat Hunting	Foresite will run Threat Hunting sessions across the Client's estate that includes information gathering, searches across the customer estate, and the generation of the automation/watchlist.
Supported Infrastructure	Windows, macOS, Linux operating systems. See specific vendor product support for the product deployed**.**
Automation (Advanced only)	Foresite will add all manual hunts, where possible, into an automated process, such as Carbon Blacks watchlists. This will enable alerting and a better security posture on the latest threats.

Customer will identify:

Critical Endpoints, Servers, Users, and/or Applications	Foresite Threat Hunting will be greatly improved by the identification of critical assets within the estate. These assets could be anything which are essential to the operation of day-to-day business, including but not limited to, Endpoints, Servers Users, and/or Applications.
Pre-Approved Actions	Clients will advise what pre-approved actions Foresite can undertake. For example, Endpoint isolation should a threat be detected, running full disk scans, first line removal attempts of a potential threat, etc.

Onboarding Stages:

Sensor Rollout	Installation of the endpoint sensors onto all Devices/Assets included within the service.

Policy Implementation	Foresite recommended policies are put in place that include individual policies for Standard Endpoints, High-value Endpoints, Standard Servers, Mission Critical Servers.
Tuning	Data and Alerts will be reviewed and tuning recommended based on Threat Hunting results, false positive alerts, customer requirements.

Patch Management

Proven, industry-leading patch management services to keep all your systems, operating systems, and third-party applications up to date with the latest software and security patches.

Most cyber-attacks involve exploits on known vulnerabilities preventable with better patch deployment. 60% of data breaches have historically involved unpatched vulnerabilities. Foresite's automated patch management solution will provide a clear picture of your security risks. By identifying non-compliant systems and reducing time-to-patch, Foresite will reduce your cybersecurity risk. Patch management process can be difficult and time consuming, but it is an essential business function Foresite can help you perfect.

Foresite's Patch Management Service is available for Windows and Linux Servers, Windows and MacOS workstations and hundreds of third-party applications. The Service is provided using Ivanti End Point Manager (EPM) and ProVision.

ProVision Patch Management includes:

Description	
ProVision Platform	✓
Reporting	✓
Ivanti EPM Software	✓
Patch related vulnerability scan (not all vulnerabilities)	✓
Automated patching based on severity and device type (e.g., workstations or servers)	✓
Auto reboots (where allowed)	✓
Patch Monitoring	✓
Patch anywhere (on prem or at home. requires internet access)	✓

Service Scope

Foresite will monitor the identified Assets in Service to keep up to date with software patches across the estate. Foresite will work with the Client to identify the Assets in scope and provide the Ivanti EPM agent for the client to install.

Patch Management Reports are available within ProVision and additional reports can be made available upon request.

All Foresite activities will be implemented remotely. In the event of issues that require physical or local access to the Device/Asset, Client may at times be required for assistance to troubleshoot.

Automation

Once configured, Patch Management is automated with the best results being achieved by keeping the automation process simple and consistent. This includes a regular patch maintenance window, ideally weekly or monthly that can be agreed on during onboarding.

Patches are deployed automatically in a staged approach to a smaller test group then after a week to the rest of the estate. This is an extra safety measure approach to capture any potential compatibility issues before full deployment.

Patch Releases

Microsoft releases their monthly patches on the second Tuesday of each month. With various standards in mind that look for patches to be installed between 14 days to 30 days after release, we start each patch cycle after patch Tuesday. Many other third-party software providers also follow this approach.

Supported Infrastructure

Windows, macOS, Linux operating systems plus most major applications such as MS Office, browsers, Adobe, and Java (see full supported applications list).

Onboarding

Foresite will work with the client to identify and bring all Devices/Assets into the Patch Management Service during the onboarding process as follows:

Pilot	One or 2 devices of each type (e.g., Server, Workstation) to prove the model and ensure there are no compatibility issues. This will involve installing the Patch Management Agent, ensuring it's reporting into the service and can deploy patches. It will test the full patch process to identify any potential issues such as firewall or app blocking. The agent is usually manually installed on these devices at this stage.
Test Group	Foresite will work with the Client to identify a group of devices (typically 10) that will receive patches first for each patching period. This test mass deployment in the Client environment using software deployment tools or group policy to install the agent remotely.

Estate Roll Out	Installation of Patch Management Agent to all infrastructure in the Service. All devices in this group will receive patches a week after the test group.

ProVision Assessment

Vulnerability Scanning

Vulnerability scans assess computers, systems, and networks for security weaknesses, also known as vulnerabilities. These scans are typically automated and give a beginning look at what could possibly be exploited.

A vulnerability scan is the first step performed in the process of conducting a vulnerability assessment. Vulnerability scans create auto-generated reports which generally detect only surface level vulnerabilities. The scans should be used in lieu of a full assessment.

Vulnerability scans are a passive approach to vulnerability management, as they don't go beyond reporting on detected vulnerabilities. Foresite follows 'NIST SP 800-115 Technical Guide to Information Security Testing and Assessment' as our testing framework.

Vulnerability Assessment Testing

A vulnerability assessment is less thorough than a penetration test, as it doesn't involve social engineering attacks or exploits designed to breach your security infrastructure.

Foresite consultants will review the results of an automated vulnerability scan, which involves a nominal amount of manual evaluation. The use of additional tools (manual testing methods) may be necessary to determine actual vulnerabilities from potential or non-existent vulnerabilities (false positives).

Any exploit that would result in a Denial of Service, disrupt services or system access, or result in the actual penetration of the system and risk damaging the system will not be performed. These vulnerabilities will be listed as potential vulnerabilities and will require further investigation. Foresite follows 'NIST SP 800-115 Technical Guide to Information Security Testing and Assessment' as our testing framework.

Penetration Testing

A penetration test simulates a hacker attempting to gain access into network infrastructures or information systems through manual (hands on) exploitation of vulnerabilities. Foresite follows 'NIST SP 800-115 Technical Guide to Information Security Testing and Assessment' as our testing framework.

Penetration testing is a manual approach performed by Foresite consultants (real people) looking to evade or overthrow the security features of system components. It is designed to exploit discovered weaknesses and determine risk exposure, giving full visibility into how malicious entities may be attacking your systems and to what extent they are at risk.

Any exploit that would result in a Denial of Service, disrupt services or system access, or result in the actual penetration of the system and risk damaging the system will not be performed. These vulnerabilities will be listed as potential vulnerabilities and will require further investigation.

PREREQUISTE

External Network Assessment activities: Delivery of services route through nodes that map back to Foresite.

Internal Network Assessment activities require network access via:

1. Onsite at the request of the customer
2. Preconfigured physical appliance, shipped and installed
3. Virtual installation of Foresite .ISO within customer environment

Customer will choose a testing method:

White-box:	Customer provides detailed information about the network, often including IP addresses/ranges, sensitive device IPs, network diagrams, and other pertinent documents.
Gray-box:	Customer provides limited information such as number of active devices, number of subnets, and IP addresses/ranges.
Black-box:	Customer provides network access to resources/equipment. No network information is provided, except static Ips.

Project Phases:

Discovery and Enumeration	a) **Fingerprinting:** Fingerprinting is the systematic discovery of a target in order to build an attack profile. With no inside knowledge of your infrastructure, Foresite will identify its access points and address ranges, determine associated domain names, attempt to gain insight into user id/password makeup, identify potential social engineering avenues, and gather information about your infrastructure. These determinations will be accomplished using publicly available information. Note that no social engineering will be attempted during this phase. Once this phase is complete, Foresite will contact your point of contact and confirm finding regarding discovered IP-address ranges. Fingerprinting is only necessary if a Black-box approach is used. b) **Host, Service, and Application Identification:** This activity includes identifying all accessible hosts and their associated services and applications within the identified IP-address ranges in their entirety.

	Where possible, identification will include system type, O/S type, services type, and service version.
Vulnerability Identification	This activity involves identifying vulnerabilities for each identified host and associated services using both public and proprietary techniques. Foresite will correlate the vulnerabilities to determine if a combination of vulnerabilities will allow for a larger exploit. We will provide a risk rating based upon technical, legal and regulatory, and business issues.
Validation and Assessment	Foresite will conduct a false positive analysis to confirm that the vulnerabilities identified via scanning are indeed actual confirmed or potential vulnerabilities. This activity will be conducted by a Foresite analyst using manual testing methods. Any exploit that would result in a Denial of Service, disrupt services or system access, or result in the actual penetration of the system and risk damaging the system will not be performed. These vulnerabilities will be listed as potential vulnerabilities and will require further investigation.
Exploitation and Penetration Testing	Penetration Testing activities may be performed on specific network segments, VLANs, or whole networks and are based on a case-by-case basis with the Customer. Penetration Testing includes exploitation and attempts to gain access via identified vulnerabilities to gather additional data or to devices. Upon gaining access to a device, Foresite will gather additional information to move laterally (if needed/required) within the environment. This may include installing tools on devices, adding user accounts, or utilization of installed software/applications for "malicious" actions. All tools and accounts to be removed upon completion of testing.

<u>Important Considerations</u>

1. Penetration testing activities have inherent risks and could cause unforeseen adverse effects in Customer environment including crashing servers, exposing sensitive data, corrupting production data, disruptions or other effects. Customer understands and accepts these risks.
2. Foresite does not engage in Denial of Service (DOS) testing unless explicitly requested and will not engage in any test which would result in a DOS.
3. Testing will be scheduled during times most conducive to your organization, and no tests which would be potentially disruptive to normal business will be conducted during business hours.
4. Unless separately defined for testing, if a web application is found within the range of tested IP(s), Foresite performs only basic unauthenticated application testing.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

ASV Scanning

Approved Scanning Vendor (ASV) scans begin with an automated enumeration process to identify all the hosts and services running in your environment. Once enumeration is complete, the manual assessment phase tests for the presence of known vulnerabilities in web-applications, system applications, networking devices, and operating systems that correlate to the enumeration results. The scan engine is regularly updated with the latest vulnerabilities.

In accordance with PCI DSS Requirement 11.2.2, merchants and service providers specifically require quarterly external vulnerability scans which must be performed by an ASV. The scan is performed from a point external to the target network so that internet-facing ports and services are assessed.

Once a passing scan is performed, an Attestation of Scan Compliance is provided for documentation.

Application Testing

Application testing will be performed in one of the following manners:

White-box:	Customer provides static application code and any necessary credentials to execute on testing,
Gray-box:	Customer provides application information and any necessary information
Black-box:	Customer provides limited information with no credentials being provided

Application Testing includes attempts at exploiting identifiable vulnerabilities within applications or APIs.

Foresite follows the Open Web Application Security Project® (OWASP) guidelines to assess applications for common vulnerabilities.

OWASP is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

OWASP Top 10 Categories are available at: https://owasp.org/www-project-top-ten/

Full OWASP checklist available at: https://github.com/tanprathan/OWASP-Testing-Checklist/blob/master/OWASPv4_Checklist.xlsx

Deliverables include a full analysis of findings and recommendations.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Mobile Application Testing

Mobile Application Testing includes attempts at exploiting identifiable vulnerabilities within mobile applications.

Foresite follows the Open Web Application Security Project® (OWASP) guidelines to assess applications for common vulnerabilities.

OWASP is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

OWASP Top 10 Categories are available at: https://owasp.org/www-project-mobile-top-10/

Deliverables include a full analysis of findings and recommendations.

A Scope of Services (SOS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Wireless Testing

Wireless testing can be performed:

Onsite	Allows consultants to map the signal strength (heat map) of wireless signal propagation. Otherwise, testing activities will be performed remotely.
Remote	Testing will be performed using an appliance / device shipped to the identified location(s).

Testing Includes:

Identifying Wireless Networks	Perform passive and active scanning to identify available "seen" and “hidden” wireless networks and determine ownership so as not to test out-of-scope networks.
Vulnerability Research	Identified and in-scope wireless networks are then tested to identify and verify vulnerabilities in preparation for exploitation.
Exploitation	Leverage identified weaknesses (vulnerabilities) in attempts to gain access to wireless assets and seek to pivot to the internal network. Network traffic is analyzed to identify potentially sensitive data traversing the wireless networks.

Reporting	Reporting captures executed methods and findings into a comprehensive document. This includes detailed technical risks, vulnerabilities and how they were found, notation of successful exploits and recommendations for remediation and implementation of appropriate security controls.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Email Phishing

Phishing is when attackers send malicious emails designed to trick people into falling for a scam. The intent is often to get users to reveal financial information, system credentials or other sensitive data.

An email phishing campaign will test employee's knowledge and compliance with security procedures and their response to social engineering exploits.

Foresite will utilize common ruses delivered via email to in-scope users attempting to gain access to sensitive information. Our host will attempt to request information such as usernames, passwords, and other sensitive information in a secure and controlled method that mimic the same types of attacks an actual hacker would use.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Phone Social Engineering

Foresite social engineers will perform typical telephone attacks against in-scope personnel designed to gain the target's confidence and convince them to perform an action or provide sensitive data to test their response to social engineering exploits.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Short Message Service (SMS) Phishing

Smishing (SMS text phishing) is a type of phishing that takes place via short message service (SMS) messages – otherwise known as the text messages that you receive on your phone through your cellular carrier. The goal of smishing here is to scam or otherwise manipulate consumers or an organization's employees to test their cybersecurity awareness.

Foresite will utilize common ruses delivered via SMS to in-scope users. These types of messages generally involve some type of content that will prompt them to click on a link. Successful execution can take the user to a website that prompts them to provide their login details or other information. The goal here is to get them to provide information that attackers can use to access personal or work-related accounts, commit identity fraud, or engage in some other type of malicious activities.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Physical Security Testing

Foresite engineers will provide onsite physical site testing including:

Physical Security Testing:	This includes general observation of physical security measures, attempts to enter the building and secure areas inside of the building without authorization using methods such as “piggybacking” (following authorized users), “jimmying” or “carding” door latches, or similar methods.
Physical Security Review:	This includes general observation of physical security measures.

Foresite personnel will not use destructive entry methods, damage property, or impersonate public safety or government officials. Foresite personnel may impersonate employees, customers or vendors in attempts to gain access to sensitive information.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (RoE) for this engagement.

ProVision Assurance

Foresite Integrated Risk Management (FIRM)

Foresite’s Integrated Risk Management module (FIRM) delivers fast, powerful, security compliance orchestration. FIRM allows your team to effortlessly manage your security and compliance in real-time providing a complete measure of your cybersecurity risk scoring, which brings clarity to important risk questions:

- Is your technology implemented correctly and actively managed by trained staff?
- Are your policies well written and covering all the bases for compliance?
- Do your security practices match your defined processes?

When used in combination with Provision Monitoring, Management, and Assessment, FIRM delivers real-time, continuous updates how your risk and compliance changes based on daily security operations:

Streamline Your Compliance	254 supported compliance standards (HIPPA, PCI DSS, ISO 27001, SIMM, StateRAMP, CMMC, SOC2, SCF, NIST 800-53 R5, NIST CSF, NIST SP, ISO 27002, FFIEC and more) giving your team measurable ways to manage risk across multiple frameworks in seconds.
Maximize Your Spend	Spend less time and money on policy reviews with automatic security policies and practices scoring.
Demonstrate Security Awareness	Compliance monitoring for ongoing risk visibility with real-time scoring making security reporting easy.
Optimize Your DevSecOps	Remove security bottlenecks with 24/7 support from integrated security operations center to align your compliance and security efforts under one umbrella.
Improve Your Security Maturity	Compliance risk assessments with action plans for risk mitigation so you can set goals for enhancing your security posture.

FIRM service features:

Automated Policy Scoring	FIRM understands your policies and scores them against our industry composite gold standards that were sourced from SANS, NIST, ISACA, and other industry leading organizations. This is done through our proprietary ML algorithms that are constantly being trained on the most current and appropriate policy wording.
Automatic Control Mapping	FIRM removes the time-consuming complexity of matching regulatory framework controls to your information (policies, procedures, evidence, etc.), reducing scope from weeks to days.
Policy Templates	FIRM includes templates for specific controls and control families.
One-to-Many Compliance Mapping	Map your current compliance framework to additional regulatory frameworks to easily meet multiple compliance reporting requirements. Plan of Action and Milestones (POA&M) can be exported into any control framework.

Vulnerability Ingestion	Vulnerability assessment is a core component of regulatory frameworks. FIRM ingests vulnerability data from ProVision or your own scanner to improve your security scoring based on your actual risks and results.
Attack Simulation	Attack simulations allow you to test your organization's policies, practices, and technology to a specific set of controls to ensure they are working as expected.
Continuous Monitoring (Requires ProVision Monitor)	FIRM's continuous risk monitoring replaces the outdated point-in-time approach to compliance. Organization's environments change and evolve by the minute. Sustainable compliance must keep up with the changes to continue to meet business objectives -FIRM meets this challenge. When combined with ProVision Monitor and Assess, you will experience unprecedented integrated risk management and visibility into your compliance objectives.
Unlimited Assessments	Perform unlimited self-assessments.

GRC Services

No matter your industry, no matter the size of your business, Foresite is here to help your organization thrive. We provide expert advice from vCISO, to gap assessment, to full attestations on many frameworks to navigate increasingly complex and rapidly changing cybersecurity compliance regulations. Our team will help ensure your business meets all the regulatory data security requirements that pertain to your industry's cyber compliance.

Small business or large enterprise, from reporting processes to understanding risks, we can help you find the cyber security compliance services that work for your specific needs.

Our expert consultants will custom-tailor a Scope-of-Services specifically for your GRC engagement.

Business Operations

Terms of Use

Access and use of Foresite products described in this service description are governed by the Foresite Order Form and Foresite Software Master Agreement available at https://foresite.com/docs/ma/.

Purchasing the Service Offering

The Service Offering is offered on a subscription basis for either a one-year or three-year term unless specifically noted as one-time on the Sales Oder Form contract. Subscription Services automatically renew for successive twelve (12) months each, unless a party gives the other party written notice of non-renewal at least thirty (30) days prior to the expiration of the then-current term, or the Contract is terminated sooner as provided in the Terms and Conditions. Foresite reserves the right to increase fees by up to five (5%) upon renewal.

ProVision Supported Vendor Technologies

FORESITE CYBERSECURITY

Version: v12.2
Date: 2023-Mar-06
Classification: Public

ProVision Portfolio	Monitor	Manage	Co-Manage		
Vendor	**MA2**	**MA3**	**MA4**	**Status**	**Ingestion**
Firewalls / Network & Security					
Palo Alto					
NGFW & VPN	Yes	Yes	Yes	Released	Syslog
NGFW Additional Functions	Yes	Yes	Yes	Released	Syslog
Prisma	Yes	No	No	Released	Syslog(CEF)/API
Panorama	Yes	Yes	Yes	Released	Syslog
Fortinet					
FW & VPN	Yes	Yes	Yes	Released	Syslog
NGFW Additional Functions	Yes	Yes	Yes	Released	Syslog
FortiAnalyzer / FortiManager	Yes	Yes	Yes	Released	Syslog
FortiWeb	Yes	No	No	Parsing Only	Syslog
SDWAN	Yes	No	No	Released	Syslog
CISCO					
ASA	Yes	Yes	Yes	Released	Syslog
Meraki (MX)	Yes	Yes	Yes	Released	Syslog
Meraki Switch	Yes	No	No	Released	Syslog
Meraki Access Points	Yes	No	No	Released	Syslog
Secure Firewall - FirePOWER / FTD	Yes	Yes	Yes	Released	Syslog
ASR / ISR (routing)	Yes	No	No	Released	Syslog
Catalyst/IOS (switching)	Yes	No	No	Released	Syslog
Nexus/XOS (switching)	Yes	No	No	Released	Syslog
WLC	Yes	No	No	Released	Syslog
Cisco Umbrella	Yes	No	No	Released	API
Cisco Netflow v9	Yes	No	No	Released	Syslog
Check Point					
NGFW & VPN	Yes	No	No	Released	Syslog(CEF)
Next Generation All Other Blades	Yes	No	No	On Req.	Syslog
Juniper					
SRX	Yes	No	No	Released	Syslog
SSG	No	No	No	EOL	Syslog
SA / MAG (Pulse SSL VPN)	Yes	No	No	Released	Syslog
EX / MX (switching / routing)	Yes	No	No	Released	Syslog
Wireless (WLC)	Yes	No	No	Released	Syslog
Sonic Wall					
Firewall (TZ & NSA Series)	Yes	Yes	Yes	Released	Syslog
Sophos					
Firewall	Yes	No	No	Released	Syslog
WatchGuard					
FireBox (FW)	Yes	No	No	Released	Syslog
Zscaler					
Zscaler ZIA	Yes	Yes	Yes	Released	Syslog(CEF)
Zscaler ZPA	No	No	No	On Req.	Syslog(CEF)
Zscaler ZDX	No	No	No	On Req.	Syslog(CEF)
Aruba					
Aruba Central	Yes	No	No	Released	API
Aruba Gateway	Yes	No	No	Released	API
ClearPass	Yes	No	No	Released	Syslog(CEF)
Airwave	Yes	No	No	Released	Syslog(CEF)
Mobility Master	Yes	No	No	Released	Syslog(CEF)
Aruba Wireless AP	Yes	No	No	Released	Syslog(CEF)
WLAN Controller	Yes	No	No	Released	Syslog(CEF)
Servers					
Windows Server	Yes	No	No	Released	Syslog (Winlogbeat)
Active Directory Server (Windows)	Yes	No	No	Released	Syslog (Winlogbeat)
Ubuntu	Yes	No	No	Released	Syslog
RHEL	Yes	No	No	Released	Syslog
Debian	Yes	No	No	Released	Syslog
Varonis DatAdvantage	Yes	No	No	Parsing Only	API
EDR/AV - Anti-Virus					
CB Defense	Yes	Yes	Yes	Released	API
Cylance	Yes	No	No	Released	Syslog
SentinelOne	Yes	Yes	Yes	Released	API
Cisco Secure Endpoint- AMP	Yes	Yes	Yes	Released	API
Bit Defender Gravity Zone	Yes	No	No	Released	API
Crowdstrike	Yes	Yes	Yes	Released	API
Cyphort	Yes	No	No	Released	Syslog
Eset	Yes	No	No	Released	Syslog(JSON)
McAfee EPO (On-Prem Only, not Cloud)	Yes	No	No	Released	Syslog(XML)
Palo Alto Cortex XDR	Yes	No	No	Released	Syslog(CEF)
Sophos Central	Yes	No	No	Released	API
Symantec End Point (SEP)	Yes	No	No	Released	Syslog
Trend Micro Deep Security	Yes	No	No	Released	Syslog(CEF)
Windows Defender for Endpoint	Yes	Yes	Yes	Released	API
Webroot AV	Yes	No	No	Released	API
SIEM / Log Management					
Splunk	Log fwd	No	No	Released	Syslog
LogRhythm	Log fwd	No	No	Released	Syslog
QRadar	Log fwd	No	No	Released	Syslog
DarkTrace	Log fwd	No	No	Released	Syslog
Authentication					
Duo	Yes	No	No	Released	API
Cisco TACACS	Yes	No	No	Released	Syslog
Cisco ISE (Identity Services Engine)	Yes	No	No	Released	Syslog
Microsoft MFA	Yes	No	No	Released	Syslog
Auth0	Yes	No	No	Released	API
Okta	Yes	No	No	Released	API
SD-WAN					
VMWare VeloCloud	Yes	No	No	Released	Syslog
Versa Networks	Soon	No	No	On Req	Syslog
Cisco Secure Firewall - Firepower SDWAN	Yes	No	No	Released	Syslog
Fortinet SDWAN	Yes	No	No	Released	Syslog
Hypervisors					
Vmware ESXi	Yes	No	No	Released	Syslog
VMWare vCenter	Yes	No	No	Released	Syslog
Nutanix	Yes	No	No	Released	Syslog
Load Balancers					
Citrix Netscaler	Yes	No	No	Released	Syslog
F5 BIG-IP (LTM only)	Yes	No	No	Limited	Syslog
Managed Vulnerability Assessment					
ProVision Integration based solution	Yes	No	No	Released	N/A
Patch Management / Ivanti	Yes	No	No	Released	N/A
PAM / DNS					
CyberArk PAM	Yes	No	No	Released	Syslog(CEF)
Infoblox	Yes	No	No	Released	Syslog
Thycotic Secret Server	Yes	No	No	Parsing Only	Syslog
Cloud					
Azure AD	Yes	No	No	Released	API
AWS	Yes	No	No	Released	API
Google Cloud	Yes	No	No	Released	API
Mail					
Office 365	Yes	No	No	Released	API
Gsuite	Yes	No	No	Released	API
Barracuda Email Security	Yes	No	No	Released	Syslog

Purchase Order
Terms & Conditions
Effective September 1, 2015

Section 1. Purchase Order.

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

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

Section 2. Performance.

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

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

Section 3. Payment and Fees.

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

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

B. Payment Timeframe.

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

C. MyFloridaMarketPlace Fees.

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

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

D. Payment Audit.

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

E. Annual Appropriation and Travel.

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

Section 4. Liability.

A. Indemnity.

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

B. Payment for Claims.

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

C. Liability Insurance.

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

D. Workers' Compensation.

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

E. Performance Bond.

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

Section 5. Compliance with Laws.

A. Conduct of Business.

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

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

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

B. Lobbying.

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

C. Gratuities.

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

D. Cooperation with Inspector General.

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

E. Public Records.

To the extent required by the Florida Public Records Act, Chapter 119, F.S., the Contractor shall maintain and allow access to public records made or received in conjunction with the Purchase Order. The Purchase Order may be terminated for cause by the Agency for the Contractor's refusal to allow access to public records.

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

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

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

Section 6. Termination.

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

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

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

Section 7. Subcontractors and Assignments.

A. Subcontractors.

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

B. Assignment.

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

Section 8. RESPECT and PRIDE.

A. RESPECT.

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

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

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

B. PRIDE.

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

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

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

Section 9. Miscellaneous.

A. Independent Contractor.

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

B. Governing Law and Venue.

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

C. Waiver.

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

D. Modification and Severability.

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

E. Time is of the Essence.

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

F. Background Check.

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

G. E-Verify.

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

H. Commodities Logistics.

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

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

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Department of
MANAGEMENT
SERVICES
We Serve Those Who Serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950

Ron DeSantis, Governor
Pedro Allende, Secretary

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT BETWEEN FLORIDA DEPARTMENT OF MANAGEMENT SERVICES AND 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-22/23-157, Security Operations Platform Solution ("Solution");

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

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

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

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

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

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

(f) State: The State of Florida.

2. **Term and Termination.** This Agreement is effective upon signature by both Parties. This Agreement may be terminated by the Department when determined to be in the best interest of the State of Florida by providing Recipient with advance written notice.

3. **Intended Third Party Beneficiary.** Customers receiving services under the Solution are intended third party beneficiaries of this Agreement, entitled to enforce any rights hereunder for their benefit.

4. **Confidential Information Use.** Use of the Confidential Information shall be limited to the provisions set forth herein and to the extent necessary to provide the services and/or commodities. The Department retains full rights and title to all Confidential Information provided by it, and any information derived therefrom. Recipient has no ownership rights to the Confidential Information provided under this Agreement, or any information derived therefrom.

5. **Recipient Obligations.** Recipient shall: 1) maintain the confidentiality of all the Confidential Information pursuant to this Agreement, as required herein, 2) comply with all federal and State laws and regulations related to information privacy and security, and 3) ensure that any Affiliates comply with the preceding two requirements as to any Confidential Information shared with or otherwise Accessed by the Affiliate. Recipient shall take all measures necessary to protect against improper Access to and/or disclosure or theft of the Confidential Information and will ensure only those individuals performing services contemplated in this Agreement will be permitted to Access the Confidential Information. Recipient shall perform the following measures to preserve the privacy, security, confidentiality, integrity, and accessibility of the Confidential Information which includes, but is not limited to:

(a) Using the Confidential Information only to provide services and/or commodities as contemplated in this Agreement and not otherwise using the Confidential Information for Recipient's own benefit or the benefit of others, or in violation of any applicable laws or regulations;

(b) Not creating derivative works based upon the Confidential Information, copying the Confidential Information, or publishing or disclosing the Confidential Information to any individual or entity except in accordance with this Agreement;

(c) Implementing and maintaining protective administrative, technical, and organizational security measures appropriate to the nature of the Confidential Information to safeguard against unauthorized Access, disclosure, or theft of the Confidential Information;

(d) Maintaining the confidentiality of the Confidential Information under this Agreement in accordance with Department policies and procedures and applicable State and federal laws and regulations;

(e) Storing and safeguarding the Confidential Information in a physically and electronically secure location where Access is limited to authorized persons;

(f) Maintaining an up-to-date list of individuals who are authorized to Access the Confidential Information;

(g) Instructing and requiring all individuals authorized to Access the Confidential Information to adhere to the confidentiality requirements set forth in this Agreement prior to being granted Access to the Confidential Information;

(h) Not allowing, through action or inaction, any Confidential Information to be sent by any medium, transmitted, or to be Accessed outside of the United States. For the purposes of this restriction, “Access” does not include remote support sessions for devices that might contain the Confidential Information; however, during the remote support session the Department requires Recipient to escort the remote support access and maintain visibility of the actions taken during the remote support access. Requests for remote access will be submitted to the Department’s Contract Manager. With approval, third parties may be granted time-limited terminal service access to information technology resources as necessary for fulfillment of related responsibilities. Remote connections are subject to detailed monitoring via two-way log reviews and the use of other tools; and

(i) Performing all actions necessary to assist with all tasks in furtherance of the Department’s efforts to comply with the obligations under Chapters 60FF and 60GG, Florida Administrative Code, as applicable.

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

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

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

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

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

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

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

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

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

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

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

FLORIDA DEPARTMENT OF MANAGEMENT SERVICES	**World Wide Technology, LLC**
DocuSigned by: By: Pedro Allende 5E91A9D309EB47C...	By: Gregory Brush Digitally signed by Gregory Brush Date: 2023.05.12 14:03:41 -05'00'
Name: Pedro Allende	Name: Gregory Brush
Title: Secretary	Title: Area Vice President, Public Sector
Date: 6/14/2023 | 5:01 PM EDT	Date: May 12, 2023