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 CONTENT DELIVERY NETWORK DMS-22/23-156B 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-22/23-156, Content Delivery Network (CDN) Solution; and

**WHEREAS**, the Department has accepted the Contractor's Quote and enters into this Contract in accordance with the terms and conditions of RFQ No. DMS-22/23-156.

**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-22/23-156;
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-22/23-156 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 Mgr
1 World Wide Way
St. Louis, MO 63146
Telephone: (314) 995-6103
Email: carol.harting@wwt.com

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

## 9.0 Assignment

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

## 10.0 Price Decreases

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

## 11.0 Additions/Deletions

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

## 12.0 Cooperative Purchasing

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

## 13.0 Other Conditions

### 13.1 Independent Contractor Status

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

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

**13.2** Force Majeure

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

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

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

**13.4** Employment of State Workers

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

**SIGNATURE PAGE IMMEDIATELY FOLLOWS**

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

ST. LOUIS BASED WORLD WIDE
TECHNOLOGY, INC.:

DocuSigned by:
E5C8AD825C76425...
Authorized Signature

Greg Brush
Print Name

AVP Public Sector
Title

6/29/2023 | 9:44 PM CDT
Date

STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES:

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

6/30/2023 | 7:39 AM EDT
Date

# Exhibit "A"

# Request for Quotes (RFQ)

# DMS-22/23-156

# Content Delivery Network (CDN) 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: A content delivery network (CDN), which is a distributed network of servers that work together to provide fast delivery of internet content, such as images, videos, HTML pages, JavaScript files, and other web assets to end-users based on their geographic location.

## 2.0 OBJECTIVE

Pursuant to section 287.056(2), F.S., the Department intends to purchase a content delivery network (CDN) Solution for use by the Department and Customers to provide fast delivery of internet content, such as images, videos, HTML pages, JavaScript files, and other web assets to end-users based on their geographic location, 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 CDN software 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 be designed to improve the performance, reliability, and scalability of delivering content over the internet. Its main purpose is to efficiently distribute web content, such as images, videos, files, and other static or dynamic resources, to end-users across different geographical locations. A Solution aims to deliver content faster, more reliably, and securely to end-users by leveraging a network of geographically distributed servers, reducing latency, enhancing availability, scaling bandwidth, and optimizing content delivery.

**6.1.1.** Security

The Solution must be designed and implemented to comply with Florida cybersecurity statutes and rules. The Solution shall have multiple layers of security, including but not limited to network and application firewalls, Distributed Denial-of-Service (DDoS) protection, Secure Sockets Layer (SSL) encryption, Secure Domain Name System (DNS), Web Application Firewall, Bot Detection and real-time threat detection and response mechanisms.

**6.1.2.** Scalability

The Solution must be scalable to meet the needs of a multi-tenant enterprise. The Solution shall have the ability to quickly add or remove resources based on demand.

**6.1.3.** Performance

The Solution must be able to deliver content quickly and efficiently to end-users. The Solution shall have multiple points of presence (POPs) to ensure that content is delivered from the closest server to the end-user.

**6.1.4.** Customization

The Solution must allow for customization of caching rules, SSL certificates, and other settings to meet the specific needs of the enterprise.

**6.1.5.** User Management

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

**6.1.6.** Content Delivery

The Solution shall be able to deliver a wide range of content types, including but not limited to static content, dynamic content, and streaming media.

**6.1.7.** Caching

The Solution shall be able to cache content at the edge to reduce origin server load and improve performance.

**6.1.8.** DDoS Protection

The Solution shall be able to protect against DDoS attacks by filtering out malicious traffic and redirecting legitimate traffic to the origin server.

**6.1.9.** Load Balancing

The Solution shall have the ability to balance traffic across multiple origin servers to ensure that no single server is overloaded.

**6.1.10.** Real-time Monitoring

The Solution shall provide real-time monitoring of traffic, usage, and security incidents.

**6.1.11.** Content Optimization

The Solution shall have tools to optimize content delivery, such as image compression and minification of HyperText Markup Language (HTML), Cascading Style Sheets (CSS), and JavaScript.

**6.1.12.** Onboarding

The Solution shall include a staging environment for onboarding and changes.

**6.1.13.** Data Restricting

The Solution shall have the ability to contain/restrict data to the continental United States.

**6.1.14.** Multi-Tenant

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

**6.1.15.** Cloud Management

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

**6.1.16.** Managed Security Services

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

**6.1.17.** Malware Prevention

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

**6.1.18.** Product Usability

The Solution shall provide easy to understand friendly interfaces with intuitive designs to facilitate user engagement.

**6.1.19.** Administration and Management Usability

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

**6.1.20.** Endpoint Protection Platform Suite

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

**6.1.21.** Operating System Support

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

**6.1.22.** Disaster Recovery and Backup

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

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

**6.1.24.** 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.

**6.1.25.** 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.

**6.1.26.** 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.

**6.1.27.** Developer tools and customization

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

**6.1.28.** Integration

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

**6.1.28.2.** The Solution shall be capable of data integration through common exchange techniques and frameworks such as RESTful Application Programming Interfaces (APIs).

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

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

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

**6.1.29.** 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.

**6.1.29.1.** 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.

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

## 6.2. Training and Support

The Solution shall include comprehensive technical support to assist with implementation, customization, and troubleshooting. 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 has 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.), 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 Contract 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 (in-person, live webinar, online course, etc.), 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, resolution times, usage, and security incidents, 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<br>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.<br>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.<br>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).<br>Monthly Implementation Reports are due five (5) calendar days after the end of the month.<br>Monthly Training Reports are due five (5) calendar days after the end of the month.<br>Monthly Service Reports are due five (5) calendar days after the end of the month.<br>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 content delivery network software 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 12, 2023 |
| Pre-Quote Conference<br>Registration Link: https://us02web.zoom.us/meeting/register/tZElceqvqz0tHtJ5CTHAPP5dXIoquUoX0FZw | May 16, 2023, at 2:00 p.m., Eastern Time |
| Responses Due to the Procurement Officer, via email | May 23, 2023, by 5:00 p.m., Eastern Time |
| Solution Demonstrations and Quote Negotiations | May 24-26, 2023 |
| Anticipated Award, via email | May 26, 2023 |

## 12.0 PROCUREMENT OFFICER

The Procurement Officer for this RFQ is:

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

## 13.0 PRE-QUOTE CONFERENCE

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

## 14.0 SOLUTION DEMONSTRATIONS

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

## 15.0 QUOTE NEGOTIATIONS

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

## 16.0 SELECTION OF AWARD

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

## 17.0 RFQ HIERARCHY

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

1) The PO(s);
2) The ATC(s);
3) The Department's Non-Disclosure Agreement (NDA) or other Purchaser's NDA;
4) This RFQ;
5) Department's Purchase Order Terms and Conditions;
6) The ACS contract the vendor submitted their Quote in accordance with [ACS: Cloud Solutions (43230000-NASPO-16-ACS), Software Value Added Reseller (SVAR) (43230000-23-NASPO-ACS), or Technology Products, Services, Solutions, and Related Products and Services (43210000-US-16-ACS); and
7) The vendor's Quote.

## 18.0 DEPARTMENT'S CONTRACT MANAGER

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

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

## 19.0 PAYMENT

**19.1** The Contractor will be compensated in advance, annually, for all Deliverables per PO. Once the Implementation Plan is approved by the Purchaser, FL[DS] (if applicable) and the Customer in writing, the Contractor shall provide the Customer with access to the software in accordance with the Final Implementation Plan. Once software access is granted to the Customer, and the Customer confirms receipt, the Contractor will submit one (1) invoice to the Contract Manager specified in the PO indicating the date the Customer received the software access.

**19.2** On each invoice, the Contractor shall certify that all costs and fees claimed in the invoice statement for payment are accurate and were performed in furtherance of the PO.

**19.3** Contractor compensation will be exclusively made in accordance with the terms of this RFQ, any applicable ATC, and the PO. The Purchaser will not reimburse the Contractor for any other expenses associated with, or related to, any applicable ATC or resultant PO(s). For example, travel related expenses, including lodging, mileage, vehicle rental, and food, will not be subject to reimbursement.

**19.4** Purchasers shall pay invoices in accordance with their governing laws and regulations, which shall govern the rights and obligations of the Purchaser and the Contractor. The Department shall pay invoices submitted by the Contractor in accordance with the provisions of section 215.422, F.S., which shall govern the rights and obligations of the Department and the Contractor.

**19.5** The Contractor is responsible for the performance of all tasks and deliverables contained in any applicable ATC or PO.

## 20.0 PUBLIC RECORDS AND DOCUMENT MANAGEMENT

### 20.1 Access to Public Records

The Department may unilaterally cancel any applicable ATC or PO for failure by the Contractor to comply with this section by not allowing access to all public records, as defined in Chapter 119, F.S., made or received by the Contractor in conjunction with any applicable ATC or PO.

### 20.2 Contractor as Agent

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

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

**RELATING TO THE PURCHASE ORDER, CONTACT THE FOLLOWING CONTACTS:**

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

**OTHER PURCHASER:**
**CONTRACT MANAGER SPECIFIED ON THE PO**

### 20.3 Public Records Exemption

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

### 20.4 Document Management

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

## 21.0 IDENITIFICATION AND PROTECTION OF CONFIDENTIAL INFORMATION

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

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

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

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

## 22.0 USE OF SUBCONTRACTORS

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

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

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

## 23.0 LEGISLATIVE APPROPRIATION

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

## 24.0 MODIFICATIONS

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

## 25.0 CONFLICT OF INTEREST

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

## 26.0 DISCRIMINATIORY, CONVICTED AND ANTITRUST VENDORS LISTS

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

## 27.0 E-VERIFY

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

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

## 28.0 COOPERATION WITH INSPECTOR GENERAL

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

## 29.0 ACCESSIBILITY

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

## 30.0 PRODUCTION AND INSPECTION

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

## 31.0 SCRUTINIZED COMPANIES

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

## 32.0 BACKGROUND SCREENING

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

### 32.1 Background Check

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

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

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

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

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

### 32.2 Disqualifying Offenses

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

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

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

### 32.3 Refresh Screening

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

### 32.4 Self-Disclosure

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

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

### 32.5 Duty to Provide Security Data

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

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

### 32.6 Screening Compliance Audits and Security Inspections

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

### 32.7 Record Retention

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

# 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 content delivery network software 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 GB** |
| 1 | **<u>Initial Software Year</u>**<br>One year of content delivery network software Solution as described in the RFQ per gigabyte (GB). To include:<br>• **Implementation**<br>• **initial training**<br>• **Initial Integration**<br>• integration maintenance<br>• support services | $ ________ |
| 2 | **<u>Subsequent Software Year</u>**<br>One year of content delivery network software Solution as described in the RFQ per GB. To include:<br>• **ongoing training**<br>• integration maintenance<br>• support services | $ ________ |

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

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

______________________________
Vendor Name

______________________________
Signature

______________________________
FEIN

______________________________
Signatory Printed Name

______________________________
Date

# ATTACHMENT B
# CONTACT INFORMATION SHEET

## I. Contact Instructions

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

## II. Contact Information

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

# The State of Florida

## Department of Management Services

## Content Delivery Network (CDN) Solution

**RFQ Number DMS-22/23-156**

Cloud Solutions (43230000-NASPO-16-ACS)

May 23, 2023

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

**wwt.com**

**May 23, 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 Content Delivery Network (CDN) 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 Content Delivery Network (CDN) Solution that optimizes web content delivery to end-users across different geographical locations and reduces latency, enhances availability, scales bandwidth and ensures security. Our solution for DMS-22/23-156 easily integrates with the goals of recently released RFQs and fortifies the Department's Enterprise Cybersecurity Resiliency Program as a world-class model for the nation.

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

For this CDN project, WWT supplies a multi-tenant architecture that manages content delivery over the internet statewide through multiple layers of security for a wide range of operating systems. Managed web content includes images, videos, files and other static or dynamic resources that can be aggregated up to a single instance and view for comprehensive visibility. Our solution incorporates DDoS protection, content optimization, malware prevention, 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 and Akamai 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 validate the effectiveness of CDN upgrades for the Department

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

We have created custom integrated labs for customers with our partners' CDN and security solutions to provide fast delivery, enhanced availability 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 CDN projects assure the success of DMS-22/23-156

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:

- Developed an Enterprise pricing model nullifying the risks and costs associated with "bit and byte" models for traffic sources, destinations, volumes and frequencies for DMS 21/22-241
- Manage more than 4,000 edge servers in Florida and 114,000 in the US for fast content delivery
- WWT partner processes trillions of internet transactions daily, serving 30% of all global traffic

WWT believes in the power of uniting employees, customers, partners and communities through secure CDN solutions. 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 CDN project to continue ensuring the safe delivery of web content to the Department 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 content delivery network software Solution proposed and how it meets the requirements of this RFQ to include the following at a minimum:**

### World Wide Technology

WWT has partnered with Foresite and Akamai for this response. WWT will ensure that all the Department's customers have a standard experience and solution delivered, a consistent user experience, level of sustainment effort as well as consistency with regards to onboarding, data/app hosting and sustainment processes.

### Foresite

The solutions proposed for Content Delivery Network (CDN) RFQ listed below all strive for high availability based on their architectures and processes attaining availability beyond the industry standard of 99.95%.  The solution architecture is hosted in the Amazon AWS environment, with multi availability zones, which meets the 99.999% uptime requirements.

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 and Elasticity:** 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 maintains two regionally diverse SOCs, and the ability, as a last resort, for our analysts to work remotely in the event both SOCs are impacted and are unreachable.

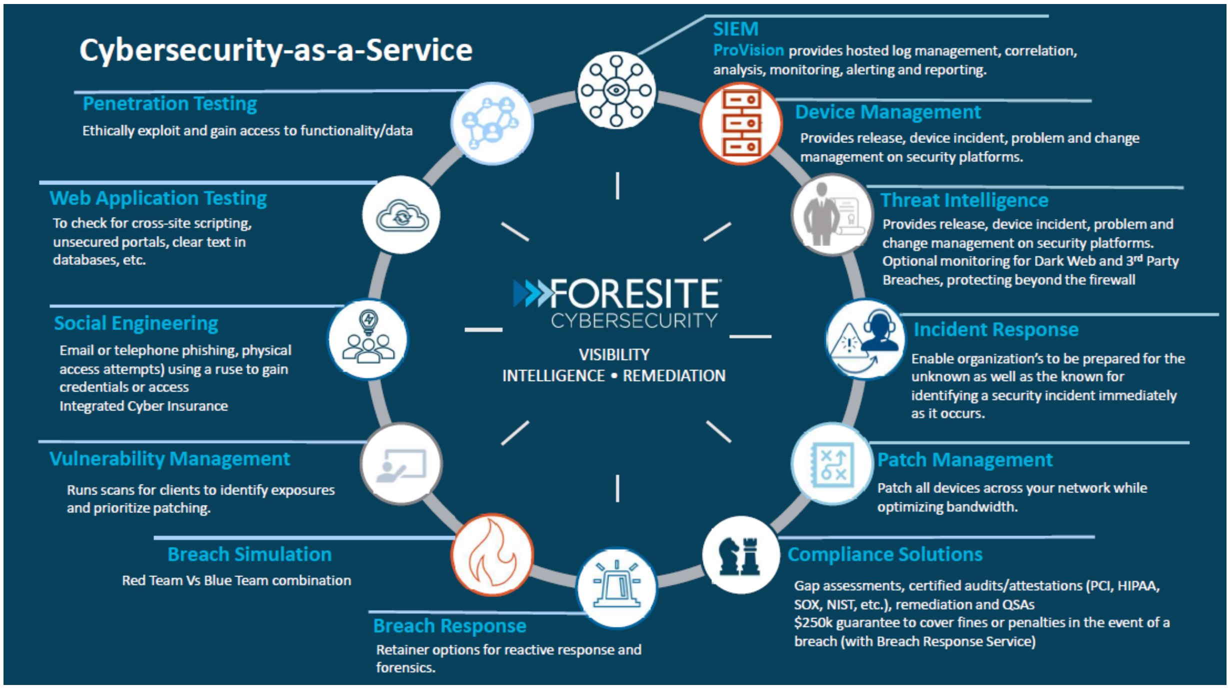
Foresite has a BCP/DR Policy that is exercised routinely and, as part of our Information Security Management System (ISMS), it is regularly audited by our external auditors, including ISO27001.

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

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

### ProVision Platform

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



Cybersecurity-as-a-Service

SIEM
ProVision provides hosted log management, correlation, analysis, monitoring, alerting and reporting.

Device Management
Provides release, device incident, problem and change management on security platforms.

Threat Intelligence
Provides release, device incident, problem and change management on security platforms.
Optional monitoring for Dark Web and 3rd Party Breaches, protecting beyond the firewall

Incident Response
Enable organization's to be prepared for the unknown as well as the known for identifying a security incident immediately as it occurs.

Patch Management
Patch all devices across your network while optimizing bandwidth.

Compliance Solutions
Gap assessments, certified audits/attestations (PCI, HIPAA, SOX, NIST, etc.), remediation and QSAs
$250k guarantee to cover fines or penalties in the event of a breach (with Breach Response Service)

Breach Response
Retainer options for reactive response and forensics.

Breach Simulation
Red Team Vs Blue Team combination

Vulnerability Management
Runs scans for clients to identify exposures and prioritize patching.

Social Engineering
Email or telephone phishing, physical access attempts) using a ruse to gain credentials or access
Integrated Cyber Insurance

Web Application Testing
To check for cross-site scripting, unsecured portals, clear text in databases, etc.

Penetration Testing
Ethically exploit and gain access to functionality/data

FORESITE CYBERSECURITY
VISIBILITY
INTELLIGENCE • REMEDIATION

**Figure 1**

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 2014. Several of the leaders in their organization previously built an earlier iteration of an MSSP and brought many key learnings forward to Foresite. The services they deliver are critical in helping customers who are typically understaffed, overwhelmed and lacking in broad security know-how. Foresite maintains a vendor agnostic approach. Foresite has a very specific focus around MSSP, Compliance and Security Consulting Services.

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

### Akamai

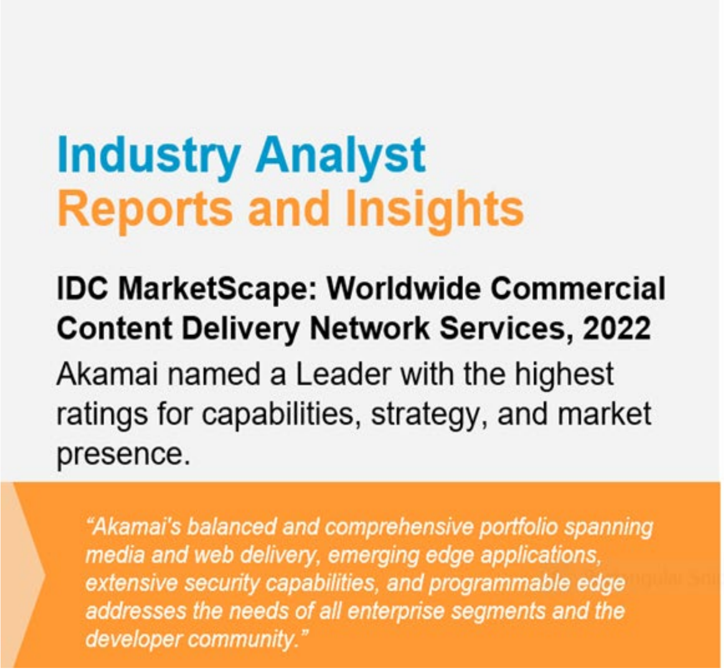
Operating the world's largest and most successful Content Delivery Network (CDN), Akamai® is the leading Cloud Security Platform providing enterprises across the globe secure, high-performing user experiences on any device, anywhere. Operational since 1998, Akamai is a profitable and financially stable company with over $3.6 billion in annual revenue, providing financial stability for both continued operations and investments in future growth and technology trends.

The highly distributed, cloud-agnostic CDN platform services for Florida agencies provide maximum levels of security, performance and availability of online agency workflows and critical apps in any environment—on-premises, across clouds, and out to the secure edge.

**Securing Web Applications, API's (WAAP) and Domain Name Services (DNS) with a comprehensive Content Delivery Network (CDN) architecture** protects web content and application programming interfaces (API) against distributed denial of service attacks and targeted web app attacks while fending off adversarial bots, detecting client-side script attacks, and protecting your users' accounts from fraud.

Additionally, platform capabilities can reduce the attack surface on websites, protect Domain Name Services distributed denial of service attacks, enhance website performance through caching and can decrease egress charges from cloud-hosted solutions.

- Built to support overall online presence for Florida government entities
- Cloud agnostic to accommodate hybrid, multi-cloud environments and the foundation for zero trust security regardless of underlying infrastructure v
- Fastest, most effective DDoS defense—at largest scale in the global market and most distributed edge infrastructure in Florida
- Non-stop availability and security of web apps and API environments with highly secure DNS
- Control cost by maximizing origin offload and reduce egress charges

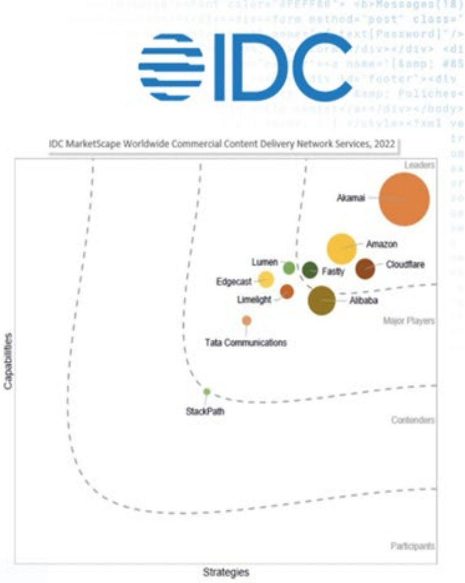


Industry Analyst
Reports and Insights

**IDC MarketScape: Worldwide Commercial Content Delivery Network Services, 2022**

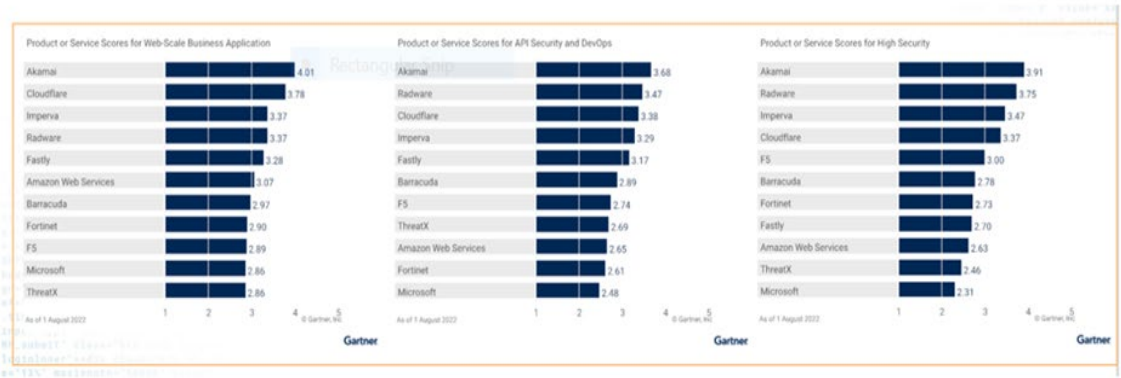
Akamai named a Leader with the highest ratings for capabilities, strategy, and market presence.

*"Akamai's balanced and comprehensive portfolio spanning media and web delivery, emerging edge applications, extensive security capabilities, and programmable edge addresses the needs of all enterprise segments and the developer community."*

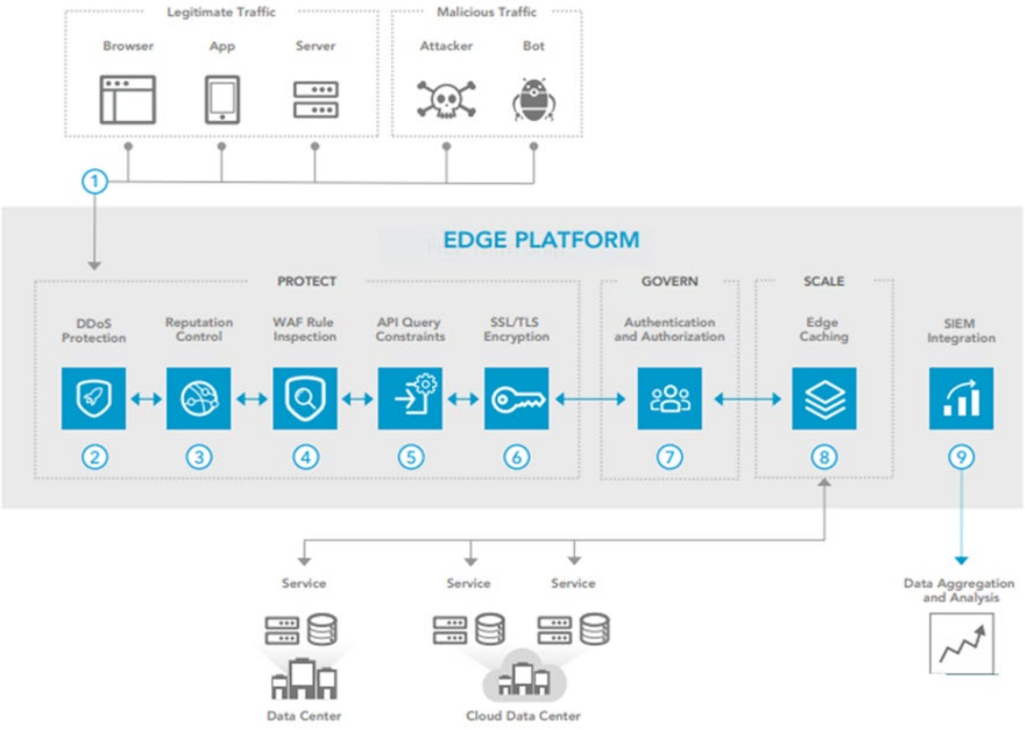


Akamai named customers' choice in **2022 Gartner® Peer Insights™ 'Voice of the Customer': Global CDN**

Akamai named customers' choice in **2023 Gartner® Peer Insights™ 'Voice of the Customer' for Cloud Web Application and API Protection**



### Example Reference Architecture by "Customer"



Below, WWT responds to each subsection of Section 6.0 Scope of Work to show how we meet the requirements of this RFQ.

### 6.1. <u>Software Solution/Specifications</u>

### 6.1.1. Security

**The Solution must be designed and implemented to comply with Florida cybersecurity statutes and rules. The Solution shall have multiple layers of security, including but not limited to network and application firewalls, Distributed Denial-of-Service (DDoS) protection, Secure Sockets Layer (SSL) encryption, Secure Domain Name System (DNS), Web Application Firewall, Bot Detection and real-time threat detection and response mechanisms.**

WWT will integrate Akamai solutions to deliver network and application firewalls, Distributed Denial-of-Service (DDoS) protection, Secure Sockets Layer (SSL) encryption, Secure Domain Name System (DNS), Web Application Firewall, Bot Detection and real-time threat detection and response mechanisms for this CDN project.

Akamai’s App & API Protector defends against DDoS, web application and API attacks and malicious bots while simultaneously allowing access to legitimate users with faster performance and improved user experience. This App & API Protector brings together web application firewall, bot mitigation, API security and Layer 7 DDoS protection into a single solution. It quickly identifies vulnerabilities and mitigates threats across your entire web and API estates — even for the most complex distributed architectures. Recognized as the leading attack detection solution on the market, App & API Protector is easy to implement and use. It delivers automatic updates for security protections and provides holistic visibility into traffic and attacks.

As a web reverse proxy platform, Akamai supports both HTTP and HTTPS traffic. This includes the ability to cache, store, and as a pass-through for sensitive information. Akamai does this by acting as a point of demarcation for the SSL/TLS, enabling Akamai to perform full-body inspection and caching of encrypted content. Furthermore, because Akamai Edge Servers maintain persistent connections, Akamai can offload the number of SSL/TLS connections to an origin. This is especially beneficial for secured transactional connections as it minimizes the impact of multiple and more resource-intensive TLS/SSL handshakes on the origin. In this scenario, the origin side Edge Server only needs to maintain a few persistent connections with the origin for transactions from multiple client-side Edge Servers connected to many client users.

Akamai delivers SSL/TLS-secured content over a network that is engineered to meet stringent standards and has been assessed, certified, and accredited under Akamai’s FedRAMP Provisional Authority to Operate (P-ATO). Additionally, Akamai’s secure delivery service meets the requirements of the OMB Mandate requiring all federal agencies to make all existing websites and services accessible through a secure connection (HTTPS only, with HSTS).

To facilitate secure and trusted transactions, Akamai provides several SSL/TLS certificate options to meet different customer business requirements. These include single hostname, wildcard, SAN, and Extended Validation certificates, as well as a seal option that displays a trust logo on the secure Web site or application.

Akamai Edge Servers can be configured to require minimum cipher strength in any SSL/TLS connection request, including FIPS-approved ciphers. Requests that do not meet the minimum can be denied or sent to an alternate page with upgrade requirements. Akamai can support the use of signed URLs and all data is encrypted.

Akamai's DNS service is a purpose-built, highly scalable and available service, supporting DNSSEC and Zone Transfer. It also provides DDoS protection for DNS infrastructure with a 100% Availability SLA.

### 6.1.2. Scalability

**The Solution must be scalable to meet the needs of a multi-tenant enterprise. The Solution shall have the ability to quickly add or remove resources based on demand.**

On average, Akamai's solution delivers web traffic averaging 180 Terabits per second (Tbps) and handles over 3.1 billion client interactions daily. Even with peaks over 260 Tbps, Akamai is able to maintain well over 60% in idle capacity. The distributed architecture of Akamai's platform provides customers with on-demand scalability to automatically meet both incremental increases and sudden spikes in traffic.

### 6.1.3. Performance

**The Solution must be able to deliver content quickly and efficiently to endusers. The Solution shall have multiple points of presence (POPs) to ensure that content is delivered from the closest server to the end-user.**

For Akamai, the definition of a POP is slightly different as Akamai's distributed architecture has no centralized or regional POPs. Essentially, every Edge Server could be considered a POP.  Akamai has 355,000 Edge Servers distributed throughout 1600 different networks. Deployments are based on demand within a geographic area, enabling Akamai to have a scalable Edge presence within an area.

Akamai is ISP and carrier-agnostic, ensuring availability by not being dependent upon a single carrier or network. Akamai Edge Servers are deployed in over 4,000 locations. Akamai leases space in most locations. Deployments can be as small as 2-4 servers, or as large as multiple racks or entire sections.

Akamai has a number of proprietary algorithms that take full advantage of its distributed architecture and are designed to operate automatically, in real-time, in the most effective and efficient manner possible. Topological measurements are continuously performed – BGP feeds from hundreds of networks are combined with real-time trace-routes and other measurements to determine the overall connectivity of the Internet. This data is merged with the latency and packet loss information collected real-time from large sampling of nodes on our network. Other data collected includes geographic location of IP addresses, latencies from numerous points on the Internet, DNS information, health of key transit regions of the Internet, and observed routing decisions. The Akamai Platform dynamically maps the entire Internet every 20 minutes determining the fastest, best available routes. Using this data, Akamai's mapping system is able to identify the best available Akamai Edge Server to connect an end-user through, and the best performing internet routes for routing connections between the end-user and origin.

To enhance performance, Akamai will always route traffic over the fastest route. To ensure availability, Akamai maps out two alternative routes, sending packets over all 3 routes. Should the primary route suddenly fail, one of the alternate routes will instantly take over. Furthermore, should the Edge Server that an end-user was initially routed suddenly before unavailable, Akamai will be able to failover to redundant Edge Server- meaning that each Edge Server is mirroring the activity of the other as a background service- without ever breaking the session.

### 6.1.4. Customization

**The Solution must allow for customization of caching rules, SSL certificates, and other settings to meet the specific needs of the enterprise.**

Akamai's solution allows for granular customization of content delivery (caching, HTTP headers, redirects, etc.), security (WAF rules, IP/Geo blocks, rate controls, etc.), the SSL certificate delivered by the Edge servers (SAN hostnames, cipher suites, etc.), and all other areas of Akamai configurations.

### 6.1.5. User Management

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

Akamai Control Center (ACC), the web interface that allows customers to manage all their Akamai configurations and settings, allows administrators to implement robust access control policies for user accounts on the system.

### 6.1.6. Content Delivery

**The Solution shall be able to deliver a wide range of content types, including but not limited to static content, dynamic content, and streaming media.**

Akamai's solution is able to deliver all HTTP content types that are supported by major browsers.

### 6.1.7. Caching

**The Solution shall be able to cache content at the edge to reduce origin server load and improve performance.**

Edge caching is the core feature of Akamai's content delivery solution.  Enabling Edge caching often leads to significant offload (i.e. reduction of origin hits), which can reduce origin egress and infrastructure costs.  Serving content to end-users directly from Edge cache also results in significant performance improvements and faster round trip times, when comparing against serving content from origin.

### 6.1.8. DDoS Protection

**The Solution shall be able to protect against DDoS attacks by filtering out malicious traffic and redirecting legitimate traffic to the origin server.**

The Akamai CDN only accepts traffic via ports 80 (HTTP) and 443 (HTTPS). All network layer (Layers 3 and 4) attacks targeting a website/application are automatically dropped at the edge. This includes traffic such as UDP Fragments, ICMP Floods, SYN Floods, ACK Floods, RESET Floods, and UDP Floods. Akamai filters through valid traffic at the network edge and automatically scales to absorb malicious traffic from volumetric attacks targeting the application layer, such as GET Floods. Protection is also provided for HTTP slow client ("drip feed") DDoS attacks, such as a Slowloris (sending partial HTTP requests that proliferate endlessly, update slowly, and never close), and RUDY (r u dead yet). The distributed nature and enormous capacity enables Akamai to mitigate attacks of several thousand times in magnitude than normal traffic loads, while maintaining site performance and availability. Also, rate control functionality of the web application firewall (WAF) further extends DDoS mitigation capabilities by detecting and mitigating against volumetric attack traffic.

### 6.1.9. Load Balancing

**The Solution shall have the ability to balance traffic across multiple origin servers to ensure that no single server is overloaded.**

Akamai's solution supports multi-origin architectures. Common load-balancing implementations leverage client request characteristics such as geography, URL being requested, or simply percentage-based.  Additional logic to maintain session affinity can also be implemented.

### 6.1.10. Real-time Monitoring

**The Solution shall provide real-time monitoring of traffic, usage, and security incidents.**

Akamai's solution includes a robust set of security monitoring tools. Security Center provides a dynamic interface enabling users to visually investigate security events. Data is displayed in real-time providing situational awareness. High-level dashboard views are available for quick security posture snapshots, and granular drill-down reports are also available for deep investigation into attack traffic.  Notifications can also be configured so that email and text alerts can be sent out in real-time as security events occur. SIEM functionality is also available to send real-time logging feeds of security events to reporting endpoints.

### 6.1.11. Content Optimization

**The Solution shall have tools to optimize content delivery, such as image compression and minification of HyperText Markup Language (HTML), Cascading Style Sheets (CSS), and JavaScript.**

Akamai's solution includes various front-end optimization features, such as:

- Adaptive Image Compression: Compresses JPEG images depending on the requesting network's performance, thus improving response time.

- Asynchronous JavaScript and Early CSS Loading: Modifies the way scripts and stylesheets are embedded into the page, making the browser process scripts, style sheets and other resources in parallel instead of forcing resources further down the page must "wait in line" until JavaScript and CSS files that appear earlier in the page are fully downloaded and executed.

- Edge CSS: Copies all the CSS links on the webpage to the top of the page in order to trigger the browser to start downloading the CSS files as early as possible. The slower the origin page and the more CSS files on the page, the higher the added value of Edge CSS. Even on fast responding origins, Edge CSS can provide better visual progress of the page just by forcing the browser to start downloading the CSS files before downloading other resources on the page. This is particularly impactful when users are accessing the pages on mobile devices where computing resources are more limited.

- EdgeStart: Allows the Edge to respond immediately with the "first part" first part of the HTML response allowing the browser to download important resources such as JS, CSS and some images sooner.

- Script Inlining: Takes external JavaScripts and inlines them in the page. This has the effect of reducing the number of requests.

- Minification: HTML, JavaScript and CSS files contain comments and whitespace that are not needed for the page's operation. Minification is the process of removing such components and reducing the total download size. Ion automatically minifies all page resources, reducing the size of pages without modifying their functionality.

- Domain Sharding: Browsers impose limits on the number of parallel connections per hostname. This leads to artificial dependencies as the browser waits for otherwise independent objects to be fully delivered before proceeding with additional requests. Domain sharding gets around this limit by distributing requests over multiple subdomains, ensuring that the browser does not hit the limit of parallel requests per hostname.

- On Demand Image Loading: Causes a page to only load the images that are visible within the current viewport. As the end-user scrolls down, new images are loaded on-demand. On-demand Image Loading helps improve page load time and reduces bandwidth for cases where an end-user doesn't actually scroll down a page.

### 6.1.12. Onboarding

**The Solution shall include a staging environment for onboarding and changes.**

Akamai's solution includes the availability of a Staging environment that can be used to test Akamai configuration changes prior to Production activation.

### 6.1.13. Data Restricting

**The Solution shall have the ability to contain/restrict data to the continental United States.**

Akamai's solution includes the ability to leverage a U.S.-only Edge Server map.

### 6.1.14. Multi-Tenant

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

Akamai's solution has support for role-based access control within Akamai Control Center (ACC), ensuring that administrator roles can be restricted if required to only have visibility and control over certain functional components within the solution.   If additional separation and view restriction is required (i.e. a multi-tenant environment), that can be achieved today using a parent/child relationship within ACC.  Parents have the ability to log in and view/modify etc. any child object.  However administrators of a child environment do not have access or visibility to other children or parents.

### 6.1.15. Cloud Management

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

N/A

### 6.1.16. Managed Security Services

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

Akamai Managed Security Services are included as an option per 6.6.1 guidelines.

### 6.1.17. Malware Prevention

**The Solution shall block malware pre-execution using the Solution's antimalware prevention program.**

It is unclear whether this was intended to be in scope for the RFQ. The service may be added as an optional offering to enhance other partner solutions for a specific customer use case. Akamai's solution is capable of malware protection, to detect and block malware in uploaded files at the edge, before it ever reaches web applications and API endpoints at origin.

1. Detects and blocks malware at the edge. Avoid the risks of scanning on your servers, where the malware could have already spread by the time it's scanned.
2. Avoids complexity and frees up your team's time. Scan files only once, rather than setting up protection in each system individually like you need to do with ICAP and agent-based scanners.
3. Positions your security posture for growth. By choosing a preventative and layered approach, you can scale your protection as your business grows, giving you extra protection at the edge even if you also want to scan again at origin.
4. Requires no changes to your applications. You do not have to configure or change application code. Malware Protection is hosted completely on the Akamai Intelligent Edge.

### 6.1.18. Product Usability

**The Solution shall provide easy to understand friendly interfaces with intuitive designs to facilitate user engagement.**

Akamai Control Center (ACC), the web-based management console, provides an easy-to-use interface for customers to manage their Akamai configurations and data reports. There is ample help text within the interface at the controls level, as well as detailed technical documentation available within the support section of ACC.

### 6.1.19. Administration and Management Usability

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

Akamai Control Center (ACC) is a web-based management console, and thus no agent is needed. The user interface is easy-to-use and highly intuitive and allows customers to perform all management tasks associated with Akamai products and configurations.

### 6.1.20. Endpoint Protection Platform Suite

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

N/A

### 6.1.21. Operating System Support

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

N/A

### 6.1.22. Disaster Recovery and Backup

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

Akamai's Information Security Program requires that Akamai engage in comprehensive business continuity and disaster recovery planning. Akamai approaches that in a decentralized and customizable means such that its operations and employee planning match the platform's highly distributed and semi-autonomous nature, constituting Akamai’s Disaster Recovery Plan (DRP).

Version control of various types of Akamai configurations (i.e. delivery, security, etc.) is enabled within the management interface.  Rollbacks can be initiated manually, however there are also internal mechanisms in place to initiate rollbacks automatically if certain error thresholds are observed during Production activations.

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

Akamai processes a variety of types of data, and confidentiality is protected in different ways depending on the data type.

With respect to content being delivered over the Akamai Edge Platform, to the extent customers configure their properties to encrypt their content in transit, Akamai will do so using the TLS version 1.3 between Akamai servers and otherwise using the TLS versions and cipher profiles configured by customers with respect to transit between Akamai and the end users and between Akamai and the origin servers.

Akamai utilizes a proprietary, distributed secret management system called KMI (Key Management Infrastructure) to securely generate, store, and deliver all secrets (including encryption keys, customer TLS certificates used on the Enhanced TLS, etc.). KMI ensures that human access to secrets is minimal, secrets are stored with AES-256 encryption, and are delivered over TLS. KMI machines are deployed in Akamai's highest security racks for physical security, with very strict access control procedures and monitoring.

### 6.1.24. 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.**

Akamai Control Center (ACC) provides the full suite of identity and access management capabilities, including user authentication, password policy management, 2FA, SSO, and RBAC.

### 6.1.25. 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.**

N/A

### 6.1.26. 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.**

Akamai was the first Content Delivery Network (CDN) to obtain a FedRAMP Moderate Joint Authorization Board P-ATO in 2013 and remains the most secure solution in the market for government agencies.  Akamai's solutions complies with a variety of global and regional information security compliance programs, such as:

- FedRAMP: The Federal Risk and Authorization Management Program, U.S. Government Cloud Service Provider Authorization
- HIPAA: Health Insurance Portability and Accountability Act, Protected Health Information
- PCI DSS: Payment Card Industry Data Security Standard
- SOC 2: System and Organization Controls 2, Type 1 and 2
- ISO 27001: International Organization for Standardization, Security Management Controls
- ISO 27017: International Organization for Standardization, Public Cloud Security Controls
- ISO 27018: International Organization for Standardization, Public Cloud Privacy Controls
- ISO 27701: International Organization for Standardization, Privacy Management Controls

https://www.akamai.com/legal/compliance

### 6.1.27. Developer tools and customization

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

https://www.akamai.com/developer

https://techdocs.akamai.com/developer/docs

https://techdocs.akamai.com/home

### 6.1.28. Integration

Example Florida Local's SOW

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

Akamai's CDN and web application security solutions are cloud-based, therefore there are no hardware or software installations required within customers' data centers or cloud implementations that would require compatibility checks. In addition, there are no additional requirements for end users to interact with web applications delivered through Akamai; those interactions would continue to function as normal through a browser or other HTTP-based client software. The SSL certificate served by Edge servers will be signed by known certificate authorities already recognized by major browsers.

The prerequisite for web application integration with Akamai is that the application must be externally available via HTTP (over ports 80/443, but non-standard ports are supported as well) and DNS. Go-live simply involves a DNS cutover to point the DNS record to an Akamai Edge hostname. There may be adjustments needed at the origin infrastructure to safely allow traffic from Akamai Edge servers to the backend application, such as the network firewall, IDP settings, etc. The Akamai managed integration team would assist in identifying any potential adjustments needed.

An additional layer of integration is enabling SIEM data feeds. Data feeds can be set up for HTTP traffic as well as attack traffic. On-premises and cloud-based SIEM tools like Splunk, QRadar, and Arcsight are supported, as well as the ability to build connectors for the SIEM app of your choice.

**6.1.28.2. The Solution shall be capable of data integration through common exchange techniques and frameworks such as RESTful Application Programming Interfaces (APIs).**

Akamai's solution provides API endpoints to manage various Akamai configurations and settings, as well as to provide data feeds for HTTP traffic logging, security events, and management events.

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

Akamai Control Center (ACC) supports SAML 2.0 integration for fully federated control of users and SSO. This solution validates the user's identity before allowing access to ACC. ACC can act as a SAML SP for SSO. Customers can use their own SAML IdP to authenticate users before entering ACC.

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

Akamai's solution includes managed integration services, which includes providing the required data feeds (HTTP logs, security events, etc.) to the state CSOC.

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

Akamai's solution includes ongoing services and support, which includes ensuring that the required data feeds to the state CSOC are functioning correctly.

**6.1.29. 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.**

Availability SLA: Akamai offers a service level("Service Level") committing to 100% availability of the contracted security service.

Performance SLA: Akamai offers a service level ("Service Level") committing that the security service will not impede origin performance in any period that the protected digital property is not under attack.

**6.1.29.1. 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.**

Please see our response above in 6.1.29.

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

If the Service fails to meet the defined service levels, the Customer will receive (as its sole remedy) a credit equal to Customer's or such domain's committed monthly security service fee for the day for the protected origin(s) in which the failure occurs, not to exceed 30 days of fees.

**6.2. <u>Training and Support</u>**
**The Solution shall include comprehensive technical support to assist with implementation, customization, and troubleshooting. 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:**

Please see draft SLA for training and support which adheres to all provisions of this RFQ.

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

Please see our response above in 6.2.

**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.), specific training suggested for each user roles.**

Please see our response above in 6.2.

**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).**

Please see our response above in 6.2.

**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.**

Please see our response above in 6.2.

**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.**

Akamai Cloud Security Solutions SLA

**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.**

Please see our response above in 6.2.3.

**6.3. Kickoff Meeting**

Akamai's managed integration services includes a kickoff meeting for each customer to review the solution, timelines, and responsibilities.

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

Akamai's solution includes managed integration services, whereby integration activities commence with a kickoff meeting between all parties.

**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.**

Akamai's solution includes managed integration services, whereby integration activities commence with a kickoff meeting between all parties.

**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.**

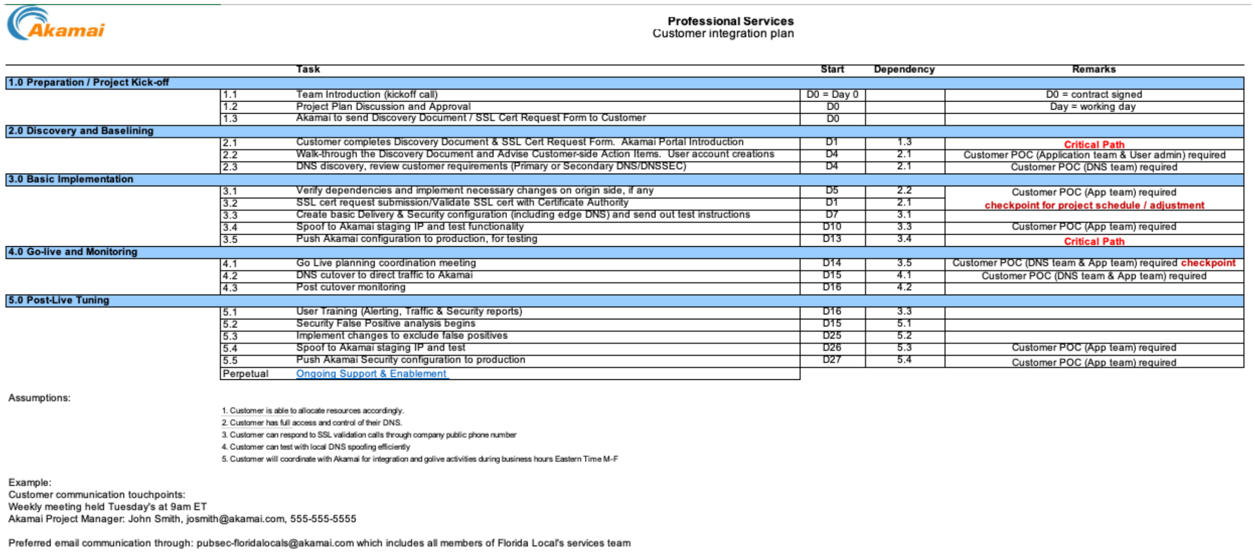
Akamai's managed integration services include demonstrations given of the solution, during the kickoff meeting or at any other point of the integration process.

## 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:**

Akamai's managed integration services includes a detailed integration plan that fulfills all the requirements listed below.



Akamai

**Professional Services**
Customer integration plan

| | | Task | Start | Dependency | Remarks |
|---|---|---|---|---|---|
| **1.0 Preparation / Project Kick-off** | | | | | |
| | 1.1 | Team Introduction (kickoff call) | D0 = Day 0 | | D0 = contract signed |
| | 1.2 | Project Plan Discussion and Approval | D0 | | Day = working day |
| | 1.3 | Akamai to send Discovery Document / SSL Cert Request Form to Customer | D0 | | |
| **2.0 Discovery and Baselining** | | | | | |
| | 2.1 | Customer completes Discovery Document & SSL Cert Request Form. Akamai Portal Introduction | D1 | 1.3 | **Critical Path** |
| | 2.2 | Walk-through the Discovery Document and Advise Customer-side Action Items. User account creations | D4 | 2.1 | Customer POC (Application team & User admin) required |
| | 2.3 | DNS discovery, review customer requirements (Primary or Secondary DNS/DNSSEC) | D4 | 2.1 | Customer POC (DNS team) required |
| **3.0 Basic Implementation** | | | | | |
| | 3.1 | Verify dependencies and implement necessary changes on origin side, if any | D5 | 2.2 | Customer POC (App team) required<br>**checkpoint for project schedule / adjustment** |
| | 3.2 | SSL cert request submission/Validate SSL cert with Certificate Authority | D1 | 2.1 | |
| | 3.3 | Create basic Delivery & Security configuration (including edge DNS) and send out test instructions | D7 | 3.1 | |
| | 3.4 | Spoof to Akamai staging IP and test functionality | D10 | 3.3 | Customer POC (App team) required |
| | 3.5 | Push Akamai configuration to production, for testing | D13 | 3.4 | **Critical Path** |
| **4.0 Go-live and Monitoring** | | | | | |
| | 4.1 | Go Live planning coordination meeting | D14 | 3.5 | Customer POC (DNS team & App team) required **checkpoint** |
| | 4.2 | DNS cutover to direct traffic to Akamai | D15 | 4.1 | Customer POC (DNS team & App team) required |
| | 4.3 | Post cutover monitoring | D16 | 4.2 | |
| **5.0 Post-Live Tuning** | | | | | |
| | 5.1 | User Training (Alerting, Traffic & Security reports) | D16 | 3.3 | |
| | 5.2 | Security False Positive analysis begins | D15 | 5.1 | |
| | 5.3 | Implement changes to exclude false positives | D25 | 5.2 | |
| | 5.4 | Spoof to Akamai staging IP and test | D26 | 5.3 | Customer POC (App team) required |
| | 5.5 | Push Akamai Security configuration to production | D27 | 5.4 | Customer POC (App team) required |
| | Perpetual | Ongoing Support & Enablement | | | |

Assumptions:

1. Customer is able to allocate resources accordingly.
2. Customer has full access and control of their DNS.
3. Customer can respond to SSL validation calls through company public phone number
4. Customer can test with local DNS spoofing efficiently
5. Customer will coordinate with Akamai for integration and golive activities during business hours Eastern Time M-F

Example:
Customer communication touchpoints:
Weekly meeting held Tuesday's at 9am ET
Akamai Project Manager: John Smith, josmith@akamai.com, 555-555-5555

Preferred email communication through: pubsec-floridalocals@akamai.com which includes all members of Florida Local's services team

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

Please see our response above for 6.4.

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

Please see our response above for 6.4.

### 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.

Please see our response above for 6.4.

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

Please see our response above for 6.4.

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

Please see our response above for 6.4.

**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.**

Please see our response above for 6.4.

**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.**

Please see our response above for 6.4.

**6.5. <u>Reporting</u>**
**The Contractor shall provide the following reports to the Purchaser:**

Standardized reports summarizing implementation status will be delivered to Customer on a monthly basis. Standardized reports summarizing delivered training will be provided to Customer on a monthly basis within 5 calendar days from the end of each month.

**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.**

Akamai’s solution includes ongoing services and support, which includes quarterly business reviews to address most relevant topics, such as the current state of service, threat reviews, and roadmap enhancement discussions with Akamai product leaders.

**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.**

Akamai’s solution includes ongoing services and support, which can include regular implementation reports to the customer at whatever frequency is desired (i.e. weekly or monthly).

**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.**

Akamai’s solution includes ongoing services and support, which can include regular training reports to the customer at whatever frequency is desired (i.e. weekly or monthly).

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

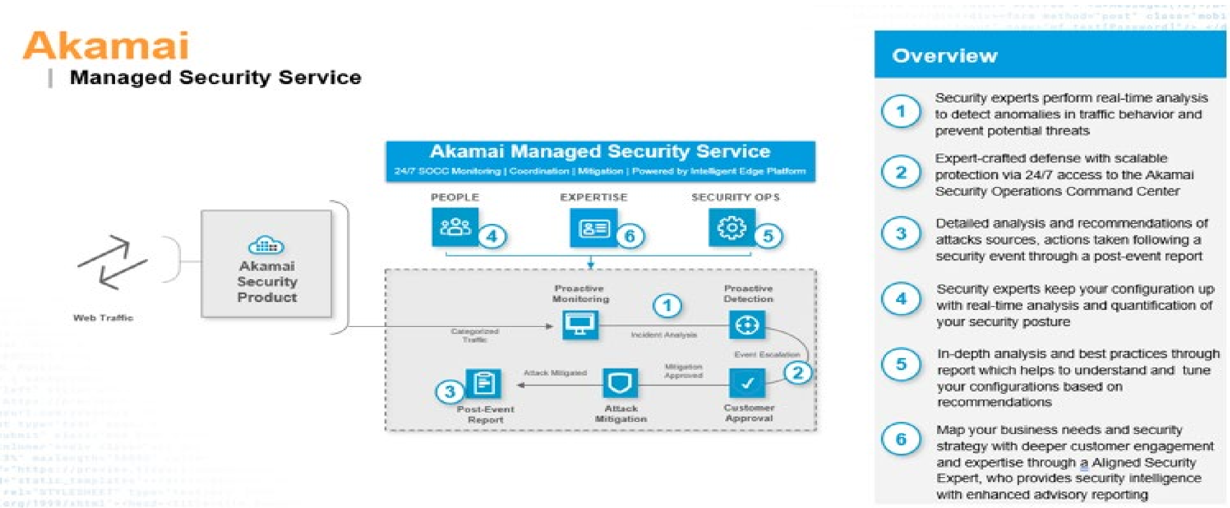
Akamai’s solution includes ongoing services and support, which can include regular service reports to the customer at whatever frequency is desired (i.e. weekly or monthly).

**6.5.5. Ad hoc reports as requested by the Purchaser.**

Akamai’s solution includes ongoing services and support, which can include ad-hoc reports requested by the customer.

**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.**

Akamai’s flagship Security Services keep Florida protected 24x7 from the most sophisticated attacks with proactive monitoring and a rapid response in the event of a cyberattack. In addition to professional services to implement necessary changes, our expert team includes aligned security advisors who deliver actionable insight through frequent contact and regular security reports.



1 Security experts perform real-time analysis to detect anomalies in traffic behavior and prevent potential threats

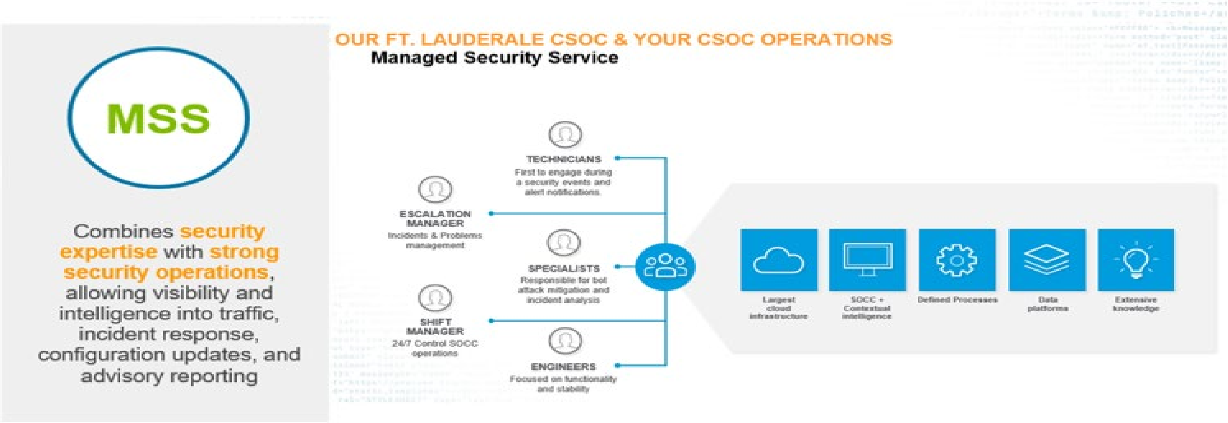
2 Expert-crafted defense with scalable protection via 24/7 access to the Akamai Security Operations Command Center

3 Detailed analysis and recommendations of attacks sources, actions taken following a security event through a post-event report

4 Security experts keep your configuration up with real-time analysis and quantification of your security posture

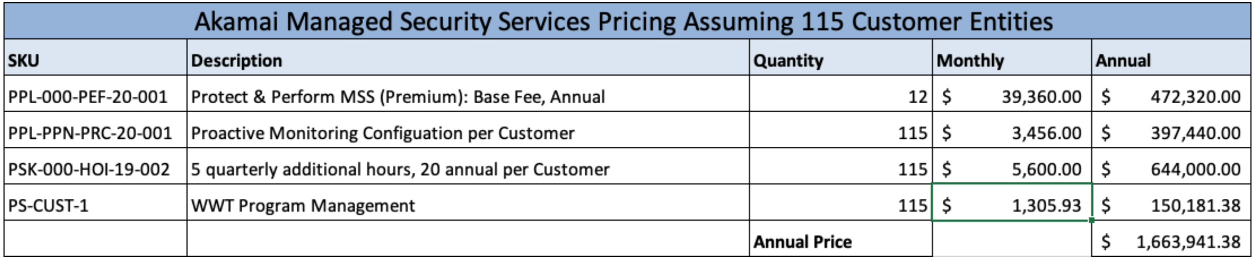
5 In-depth analysis and best practices through report which helps to understand and tune your configurations based on recommendations

6 Map your business needs and security strategy with deeper customer engagement and expertise through a Aligned Security Expert, who provides security intelligence with enhanced advisory reporting


MSS
OUR FT. LAUDERALE CSOC & YOUR CSOC OPERATIONS
Managed Security Service
TECHNICIANS
First to engage during a security events and alert notifications.
ESCALATION MANAGER
Incidents & Problems management
SPECIALISTS
Responsible for bot attack mitigation and incident analysis
SHIFT MANAGER
24/7 Control SOCC operations
ENGINEERS
Focused on functionality and stability
Largest cloud infrastructure
SOCC + Contextual intelligence
Defined Processes
Data platforms
Extensive knowledge

Combines security expertise with strong security operations, allowing visibility and intelligence into traffic, incident response, configuration updates, and advisory reporting

### Example MDR Pricing for 115 Customer Entities



Akamai Managed Security Services Pricing Assuming 115 Customer Entities

| SKU | Description | Quantity | Monthly | Annual |
|---|---|---|---|---|
| PPL-000-PEF-20-001 | Protect & Perform MSS (Premium): Base Fee, Annual | 12 | $ 39,360.00 | $ 472,320.00 |
| PPL-PPN-PRC-20-001 | Proactive Monitoring Configuation per Customer | 115 | $ 3,456.00 | $ 397,440.00 |
| PSK-000-HOI-19-002 | 5 quarterly additional hours, 20 annual per Customer | 115 | $ 5,600.00 | $ 644,000.00 |
| PS-CUST-1 | WWT Program Management | 115 | $ 1,305.93 | $ 150,181.38 |
| | | **Annual Price** | | $ 1,663,941.38 |

### Proactive Monitoring

Visibility into online activity is essential for early threat detection.

- 24/7 monitoring and anomaly detection: Security experts perform real-time analysis to detect anomalies in traffic behavior and prevent potential threats

### Security Event Management

Once a threat is identified, it’s vital to have experts available for a quick response to mitigate an attack.

- Attack support: 24/7 access to SOCC for attack support and incident response • Response service-level agreement: Security experts respond in 30 minutes or less, depending on issue severity
- Postevent report: Security experts provide a detailed, in-depth, postmortem report highlighting the attack behaviors and the actions taken following an attack or security incident.

**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.**

WWT, Foresite, and Akamai accept and will adhere to the SLA consequences listed in FL[DS] – RFQ DMS-22/23-156.

**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.**

Please see our response above in 6.6.1.

**6.6.2. <u>Future Integrations</u>**
**If available, the vendor shall provide optional pricing along with an SLA for Application Programming Interfaces available for the Solution.**

### Malware Protection

Malware Protection, an optional configuration in Akamai’s App & API Protector portfolio, protects web apps and APIs from malicious file uploads by scanning the files at the edge and not allowing them onto your corporate systems where they can spread malware. This brings a preventative solution to a growing problem as identified by OWASP — attackers embedding malware into uploaded files as organizations increasingly rely on uploads to validate information and facilitate transactions.  Described in 6.1.17.

## Edge DNS

Edge DNS is a cloud-based DNS solution that provides 24/7 DNS availability, improves DNS responsiveness, and has the resilience to defend against the largest DDoS attacks. Built on a globally distributed anycast network, it can be implemented as a primary or secondary DNS service, replacing or augmenting existing DNS infrastructure as needed.  Akamai has included Edge DNS to support the general deployment of the CDN architecture as required.  A pricing table for additional Zones with unlimited DNS queries, traffic, etc. has been included for convenience.

## Secure Internet Access

***In support of Prohibited Applications on Government-issued Devices (SB 258) / Technology in K-12 Public Schools (HB 379)***

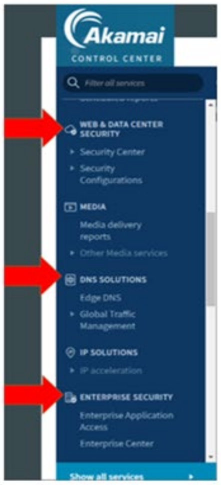
**Securely connect users & unlimited devices to the internet:** Malicious Domain Blocking & Reporting upgrade to enterprise capabilities.  The basic capability designed by the Center for Internet Security (CIS) in partnership with the Cybersecurity and Infrastructure Security Agency (CISA) and Akamai serves to prevent IT systems from connecting to harmful web domains, helping government limit infections related to known malware, ransomware, phishing, and other cyber threats.

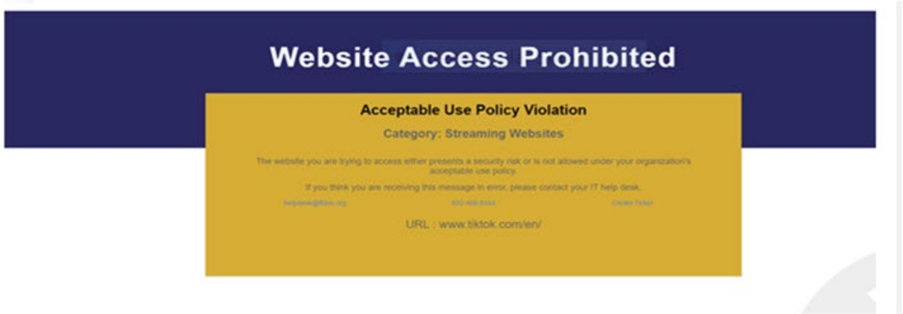
By moving to a full Secure Web Gateway (SWG) it provides real-time enterprise capabilities to protect Florida government networks users.  Built on the global Akamai Intelligent Edge Platform and Akamai's carrier-grade recursive DNS service, Secure Internet Access Enterprise is a quick-to-configure and easy-to-deploy cloud-based SWG that requires no hardware to be installed  and maintained. Secure Internet Access Enterprise has multiple layers of protection that leverage real-time Akamai cloud security intelligence and multiple static and dynamic malware-detection engines to proactively identify and block targeted threats such as malware, ransomware, phishing, and DNS-based data exfiltration.

Akamai's portal enables your security teams to centrally create, deploy, and enforce both unified security policies and acceptable use policies (AUPs) in minutes for all users, wherever they are connected to the internet. Secure Internet access protection is provided whether users are in the office or working remotely. Secure Internet Access Enterprise is powered by real-time threat intelligence based on Akamai's unrivaled global insights into internet and domain name system traffic and multiple malware-detection engines.  Includes capabilities for MDR / Security Information and Event Management (SIEM) integration technically aligned with the FLDS CSOC architecture. SIEM / MDR integration API also allows cities and county government entities to capture event details generated by Akamai security products and incorporate those details into their own third-party components at the local level.

As an FL[DS] branded offering, Akamai would be able to provide all 24x7x365 logged data to the State Security Operations Center (CSOC) based on selected intervals in accordance with FLDS data sharing policies.  This data can be analyzed and used to enrich threat intelligence reporting for each Florida government entity that uses the service as well as the state at large.  Simple pricing model for unlimited traffic and device endpoints.

Available option in the familiar Akamai console, arrow 3.




Website Access Prohibited

Acceptable Use Policy Violation

Category: Streaming Websites

The website you are trying to access either presents a security risk or is not allowed under your organization's acceptable use policy.

If you think you are receiving this message in error, please contact your IT help desk.

[illegible] [illegible] Create Ticket

URL : www.tiktok.com/en/

https://www.akamai.com/products/secure-internet-access-enterprise

https://techdocs.akamai.com/etp/docs

**Prolexic**

Although not in scope for the RFQ, a question was asked about capabilities. Given the urgency around the current project, Akamai is not complicating the response with services likely part of the scope of MyFloridaNet-2. Should this become a requirement in the future, information is included.

Akamai Prolexic is a cloud-based DDoS scrubbing platform, It available as an always-on or on-demand service, contains a Network Cloud Firewall, and offers flexible integration models based on desired security posture across hybrid origins. Prolexic is backed by a proven platform with more than 20 Tbps of dedicated DDoS defense capacity and our 24/7/365 global SOCC for a fully managed solution.

https://www.akamai.com/products/prolexic-solutions

**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.**

Edge DNS SLA

SIA SLA

**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.**

Please see our response above in 6.6.2.1.

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

WWT, Foresite, and Akamai accept and will adhere to the SLA consequences listed in FL[DS] – RFQ DMS-22/23-156.

AAP Description

AAP SLA

Akamai Cloud Security Solutions Service Level Agreements

**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, and Akamai accept and will adhere to the SLA consequences listed in FL[DS] – RFQ DMS-22/23-156.

### 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.

### Akamai

Training is included in the base cost of the CDN service giving users access to Akamai Academy. All training is self-paced.

**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.

Solution 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.

WWT will provide dedicated project management and technical expertise to ensure the solution is successfully deployed throughout the enterprise.

The following roles are included in the implementation plan:

| Role | Responsibility |
|---|---|
| Project Manager | Oversees the project; ensures timely delivery of all tasks and documentation |
| Project Coordinator | Facilitates scheduling and tracks day to day activity |
| Principal Security Consultant | Leads security solution training sessions and provides mentorship to customers' technical teams. |
| Senior Security Consultant | Provides technical guidance for security solution deployment and configuration |
| Senior Security Architect | Dedicated engineer to handle onsite and remote deployment activities (Optional renewal) |

If awarded multiple projects, WWT will consolidate roles to provide additional cost savings to the state.

This implementation schedule can be adjusted to suit the needs of FLDS and the entities participating in the cyber program.

| Team Definitions | |
|---|---|
| Teams Defined | FLDS Service Experience Team<br>FLDS Cyber Operations Team<br>WWT Sales<br>WWT Implementation<br>Foresite Team |
| Groups Defined | **Pre-Sales Team:**<br>• FLDS Service Experience Team<br>• WWT Sales<br>**Implementation Team:**<br>• FLDS Service Experience Team<br>• WWT Sales<br>• WWT Implementation Team<br>**Post Implementation Team:**<br>• FLDS Service Experience Team<br>• WWT Sales<br>• 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:<br>• Demonstrations to drive interest.<br>• Technical Q&A sessions to provide answers to any outstanding questions. | Lead:<br>• FDLS Service Experience Team<br>• WWT Sales |

| | | |
|---|---|---|
| FDLS Questionnaire | Review and complete the FLDS questionnaire | Lead:<br>• Customer |
| | Review completed questionnaire and mark agency as "READY" | Lead:<br>• FLDS Service Experience Team |

| **Implementation Activities and Tasks** | | |
|---|---|---|
| Call Schedule | Schedule a series of calls for implementation | Lead:<br>• FDLS Service Experience Team<br>Included:<br>• WWT PM |
| Call One<br><br>Estimated Duration: 60 Minutes | Walk through implementation steps:<br>a) Configuration Needs<br>i) Review FW rules, DNS configuration, others<br>b) Change Management process<br>c) Key Agency Contacts (see examples below)<br>i) Network Administrator<br>ii) IPAM Administrator<br>iii) FW Administrator<br>d) Deployment schedule small test group, larger test group, full roll out<br>e) Escalation path | Lead:<br>• Implementation Team<br>Include:<br>• Foresite<br>• FLDS Service Experience Team |
| Call Two<br><br>Estimated Duration: 30 Minutes | Configure and Troubleshoot Solution, if necessary | Lead:<br>• FLDS Cyber Operations Team<br>Include:<br>• Implementation Team |
| Learning Sessions (Up to 4 Sessions)<br><br>Estimated Duration: 60 Minutes Each | Conduct Learning Sessions:<br>• One Solution Overview and Basic Tutorial<br>• One Intermediate Tutorial<br>• One Advanced Tutorial<br>• One Additional learning session as needed.<br>• Implementation Team to discuss with customer meeting scheduling and flow.<br>• No more than 4 learning sessions total per week | Lead:<br>• Implementation Team<br>Include:<br>• FLDS Service Experience Team |
| Deploy Test Group | Test Group Deployment (per agency) | Lead:<br>• WWT Implementation Team<br>Include: |

| | | |
|---|---|---|
| | | • Implementation Team |
| Call Three<br>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:<br>• Implementation Team<br>Include:<br>• Post Implementation Team |
| Call Four<br>Estimated Duration: 60 Minutes | Review results and impact of larger group deployment, trouble shoot and setup full deployment. | Lead:<br>• Implementation Team<br>Include:<br>• Post Implementation Team |
| Call Five<br>Estimated Duration: 60 Minutes | Managed Services Onboarding:<br>• Review primary customer agency contacts<br>• Review escalation procedures<br>• Review managed services rules of engagement (device/system exclusions, authorized automated actions, authorized remediation, etc.) | Lead:<br>• Foresite<br>Include:<br>• Post Implementation Team<br>• Customer Agency |
| Call Six<br>Estimated Duration: 60 Minutes | Review full deployment, platform overview | Lead:<br>• FLDS Service Experience<br>Include:<br>• Foresite |
| Call Seven<br>Estimated Duration: 30 - 60 Minutes | OEM-specific Calls<br>• Walk through any outstanding features/capabilities required for the solution | Lead:<br>• FLDS Service Experience<br>Include:<br>• Foresite |
| Call Eight<br>Estimated Duration: 60 Minutes | Review full deployment:<br>• Discuss progress<br>• Close any open items<br>• Identify and address gaps in solution | Lead:<br>• FLDS Services Experience<br>Include:<br>• WWT Sales<br>• Foresite<br>• Implementation Team |

| **Post-Deployment and Value Calls** | | |
|---|---|---|
| Individual Agency Calls | Per agency value calls | Lead: |

| | | |
|---|---|---|
| Estimated Duration: 30 - 60 Minutes | | - FLDS Services Experience<br>Include:<br>- WWT Sales<br>- Foresite |

Please also see our response above in Section 6.4.

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

Please refer to the response for section 6.1.28 above.

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

WWT, Foresite, and Akamai accept and will adhere to the SLA consequences listed in FL[DS] – RFQ DMS-22/23-156.

### World Wide Technology

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.

### Akamai

Please refer to the response in section 6.6.2 above.

**f. A draft disaster recovery plan per section 32.5.**

WWT, Foresite, and Akamai accept and will adhere to the SLA consequences listed in FL[DS] – RFQ DMS-22/23-156.

### World Wide Technology

The solutions proposed for Content Delivery Network (CDN) 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:** 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.

### Akamai

Akamai servers are across the United States and worldwide. Upon an executed NDA Akamai can furnish Akamai's Business Continuity and Disaster Recovery Plans document.

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

### Foresite

Foresite Cybersecurity has been performing Managed Security Services that include Foresite 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 services for FL[DS].

### Akamai

**Akamai Connected Cloud** — our massively distributed edge and cloud platform — makes it easy for businesses to develop and run applications and workloads, while we put experiences closer to users and keep threats farther away. That’s why innovative companies worldwide choose Akamai to build, deliver, and secure their digital experiences.

Akamai has significant experience in delivering projects of similar or greater size.   A detailed overview of results across our private sector and government agencies as requested by the State is provided below.

### Akamai Is Trusted by:

- 45 of the top 50 brokerages
- All top 10 video streaming services
- 19 of the top 20 video game companies
- 16 of the top 20 banks
- All top 10 software companies
- 16 of the top 20 retail companies
- 13 of the top 20 healthcare providers
- 8 of the top 10 telecommunications carriers
- 8 of the top 10 healthcare payers
- 7 of the top 10 automotive companies
- 7 of the top 10 fintech companies
- 7 of the top 10 pharma companies
- All 6 U.S. military branches
- 14 of 15 U.S. federal civilian cabinet agencies
- 274 current Federal projects
- 3,000+ SLTT government entities including the largest state and the top 3 largest cities

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

### Foresite

Foresite Cybersecurity has been performing Managed Security Services that include Foresite 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 services for FL[DS].

### Akamai

The following are examples related to how Akamai has successfully delivered three different Government Agencies that span similar services identified in this RFQ for both onboarding as well as ongoing support.

### DEPARTMENT OF HOMELAND SECURITY (DHS)

Currently, over 100 DHS websites leverage Akamai's content and application delivery service. By utilizing the Akamai platform, DHS can offload approximately 90% of public Internet HTTP/HTTPS traffic from the DHS origin infrastructure.  With scale on-demand, the Akamai Intelligent Edge solution supports DHS' ~35% year-over-year growth without the need for origin infrastructure build-out.

Akamai provides DHS with the following key benefits:

- Capacity on-demand to reliably meet peak Web traffic
- Accelerated Website performance for highly interactive content
- Device-specific content adaptation
- Secure delivery of TLS-protected site content
- Reduced IT investment and operating cost by leveraging Akamai's globally distributed infrastructure for scalability, availability, and performance

Akamai has served as DHS' trusted cloud services provider and extension of the security expertise for over 10 years. Akamai is proud to have supported DHS's mission by providing 100% availability and unprecedented scalability at times of national need.

### SECURITIES AND EXCHANGE COMMISSION (SEC)

Akamai provides a FedRAMP accredited high performance and secure CDN service to the SEC. The SEC delivers ~ 100 Terabytes of material to the public every month through Akamai's Intelligent Edge Platform with the public accessing SEC websites and webcast streams for critical financial information 24 hours a day, 7 days a week, 365 days a year. By utilizing the Akamai Intelligent Edge, the SEC can offload approximately 70% of public Internet HTTP/HTTPS traffic from the SEC origin infrastructure and accommodate unpredictable load increases.

With scale on-demand, the Akamai solution supports SECs 50% year-over-year growth without the need for origin infrastructure build-out. In addition to the performance, availability and scalability benefits of the implemented solution, the SEC relies on Akamai for protection from security threat agents. Akamai's distributed computing platform protects the SEC Web infrastructure from DDoS and Web application attacks including SQL injections and Cross Site Scripts (CSS), thereby significantly improving the overall security posture of the SECs Web presence. Akamai's Professional Services meets regularly with the SEC SOC team providing ongoing recommendations for SEC to better protect itself from current and zero-day threats.

### UNITED STATES AGENCY FOR GLOBAL MEDIA (USAGM)

Akamai provides a FedRAMP accredited high performance CDN, DNS, load balancing, and security services to the USAGM, an independent agency of the United States government responsible for all nonmilitary, international broadcasting sponsored by the U.S government. Akamai's past performance on the USAGM contract demonstrates relevant capability and capacity to deliver on the solution proposed in this document. Since Akamai has been delivering rich media and accelerating content delivery to the USAGM's globally distributed user base, while protecting USAGM sites from malicious activity.

The USAGM relies on the unparalleled global presence of Akamai's network to deliver content to its end users in countries with poor Internet connectivity but high demand for USAGM's content. The agency can do this while pioneering attractive media formats such as iPhone streaming and delivery to mobile phones. The USAGM delivers nearly 300 Terabytes of material to the public every month through Akamai's Intelligent Edge Platform. Akamai's globally distributed platform delivers rich and interactive media such as portals, blogs and RSS feeds from Akamai Edge servers that are in physical proximity to USAGM end users.

Akamai's dynamic mapping system directs end-user requests to the optimal Edge server depending on their network location and load across the Akamai platform. Patented connection optimization techniques are used to improve communications between the Akamai Edge servers and the USAGM data centers, efficiently accelerating the delivery of dynamic content from data centers to end users. The USAGM also relies heavily on Akamai for protection from political hacktivism threat agents, such as Distributed Denial of Service (DDoS) attacks, while ensuring 100% availability for the agency's overseas audience.

### Additional State & Local Projects (CDN/Cloud WAF)

Florida, California, Massachusetts, Illinois, Michigan, Virginia, Iowa, New York City

**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

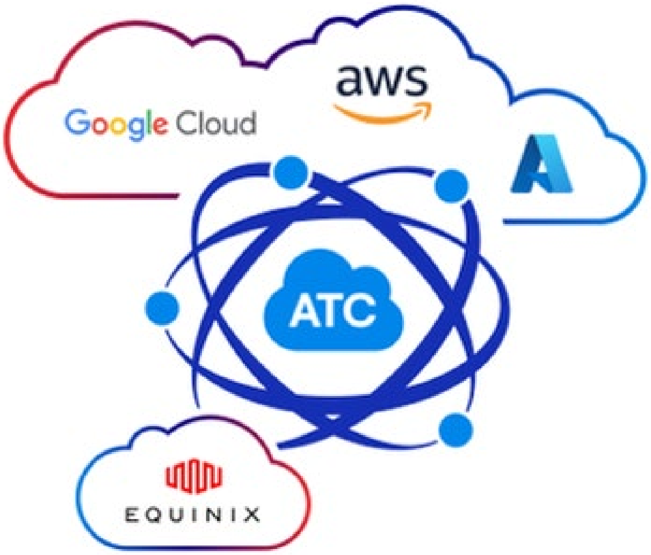
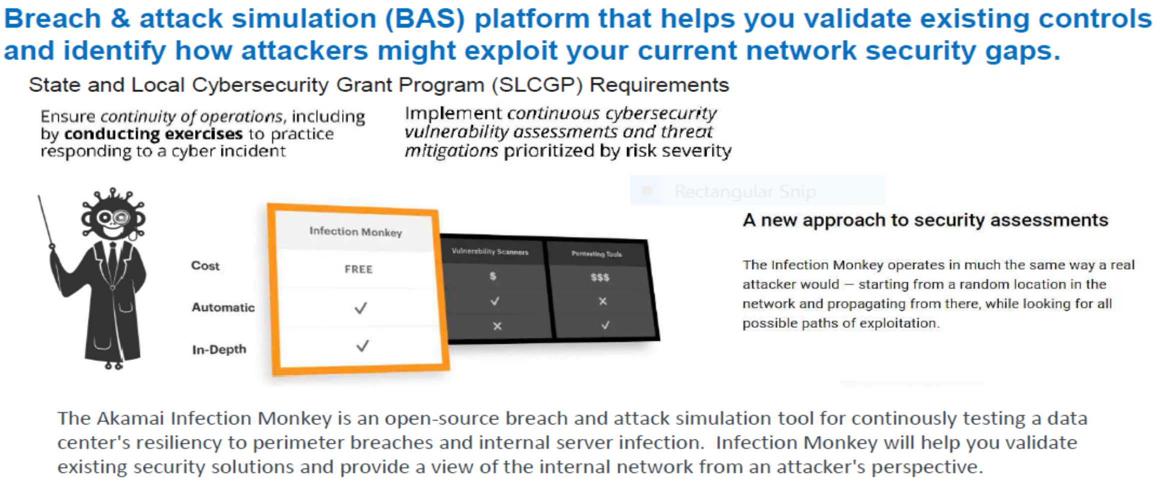


**Figure 1**
**The ATC infrastructure facilitates fast proofs of concept for current and future use cases.**

### Akamai

Below are the no-cost (free), value-added services that Akamai is offering in this RFQ.

### Breach and Attack Simulation (BAS) Platform



**Breach & attack simulation (BAS) platform that helps you validate existing controls and identify how attackers might exploit your current network security gaps.**

State and Local Cybersecurity Grant Program (SLCGP) Requirements

Ensure *continuity of operations*, including by **conducting exercises** to practice responding to a cyber incident

Implement *continuous cybersecurity vulnerability assessments and threat mitigations* prioritized by risk severity

|  | Infection Monkey | Vulnerability Scanners | Pentesting Tools |
|---|---|---|---|
| Cost | FREE | $ | $$$ |
| Automatic | ✓ | ✓ | × |
| In-Depth | ✓ | × | ✓ |

A new approach to security assessments

The Infection Monkey operates in much the same way a real attacker would – starting from a random location in the network and propagating from there, while looking for all possible paths of exploitation.

The Akamai Infection Monkey is an open-source breach and attack simulation tool for continously testing a data center's resiliency to perimeter breaches and internal server infection. Infection Monkey will help you validate existing security solutions and provide a view of the internal network from an attacker's perspective.

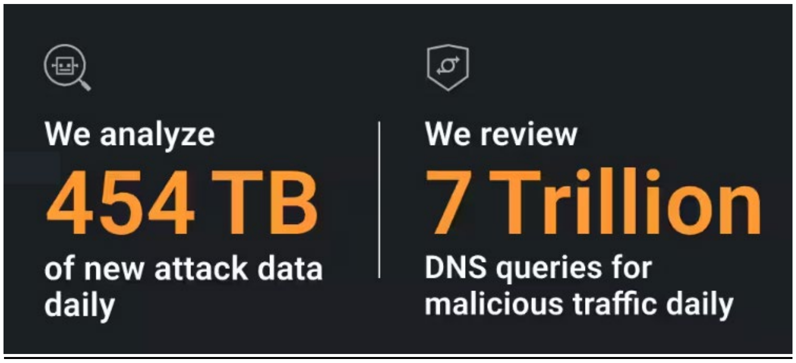
Infection Monkey is free and can be downloaded from our homepage.

https://techdocs.akamai.com/infection-monkey/docs/welcome-infection-monkey

Akamai will conduct two (2) Infection Monkey educational webinars in year 1 and record for continuing education.

**Akamai Security Intelligence Group**
In addition to the specific training and enablement plan for the RFQ deliverables, prior to September 30, 2023, Akamai will host a tour (onsite and virtual) of our Ft. Lauderdale CSOC.  Our industry experts will speak to Florida government leaders about threat intelligence, actionable insights, and the latest security news.

https://www.akamai.com/security-research



We analyze
454 TB
of new attack data daily

We review
7 Trillion
DNS queries for malicious traffic daily

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

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

**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, and Akamai accept and will adhere to the SLA consequences listed in FL[DS] – RFQ DMS-22/23-156.

**Akamai**

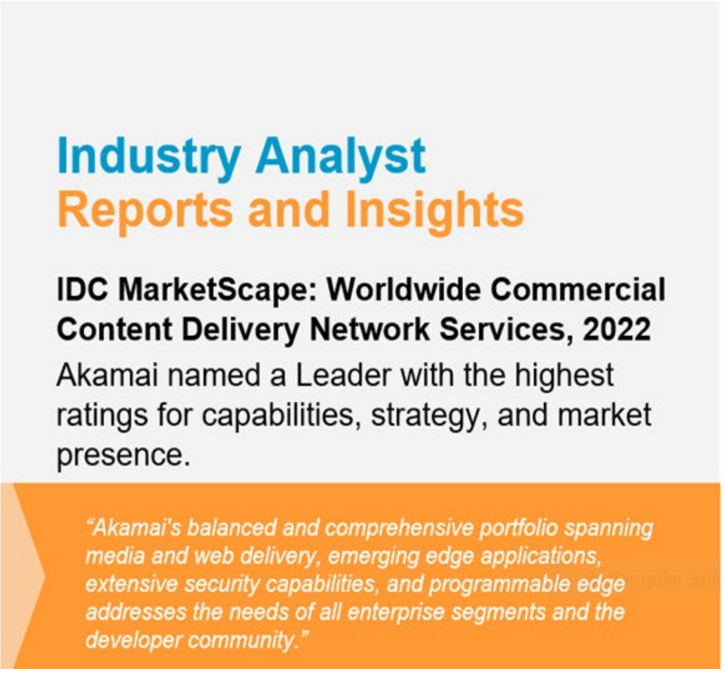
Operating the world’s largest and most successful Content Delivery Network (CDN), Akamai® is the leading Cloud Security Platform providing enterprises across the globe secure, high-performing user experiences on any device, anywhere.  Operational since 1998, Akamai is a profitable and financially stable company with over $3.6 billion in annual revenue, providing financial stability for both continued operations and investments in future growth and technology trends.

The highly distributed, cloud-agnostic CDN platform services for Florida agencies provide maximum levels of security, performance and availability of online agency workflows and critical apps in any environment—on-premises, across clouds, and out to the secure edge.

**Securing Web Applications, API’s (WAAP) and Domain Name Services (DNS) with a comprehensive Content Delivery Network (CDN) architecture** protects web content and application programming interfaces (API) against distributed denial of service attacks and targeted web app attacks while fending off adversarial bots, detecting client-side script attacks, and protecting your users' accounts from fraud.

Additionally, platform capabilities can reduce the attack surface on websites, protect Domain Name Services distributed denial of service attacks, enhance website performance through caching and can decrease egress charges from cloud-hosted solutions.

- Built to support overall online presence for Florida government entities
- Cloud agnostic to accommodate hybrid, multi-cloud environments and the foundation for zero trust security regardless of underlying infrastructure v
- Fastest, most effective DDoS defense—at largest scale in the global market and most distributed edge infrastructure in Florida
- Non-stop availability and security of web apps and API environments with highly secure DNS
- Control cost by maximizing origin offload and reduce egress charges

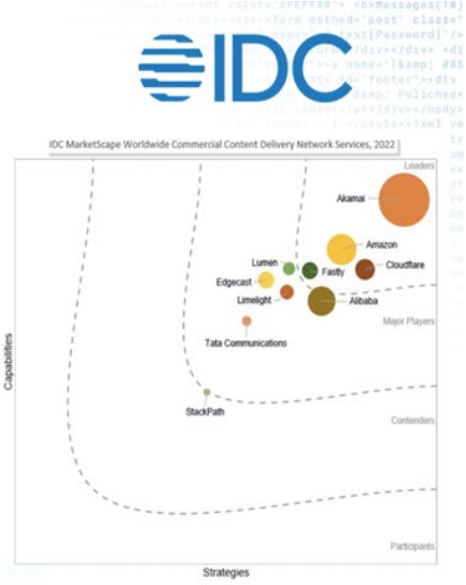


Industry Analyst
Reports and Insights

IDC MarketScape: Worldwide Commercial Content Delivery Network Services, 2022

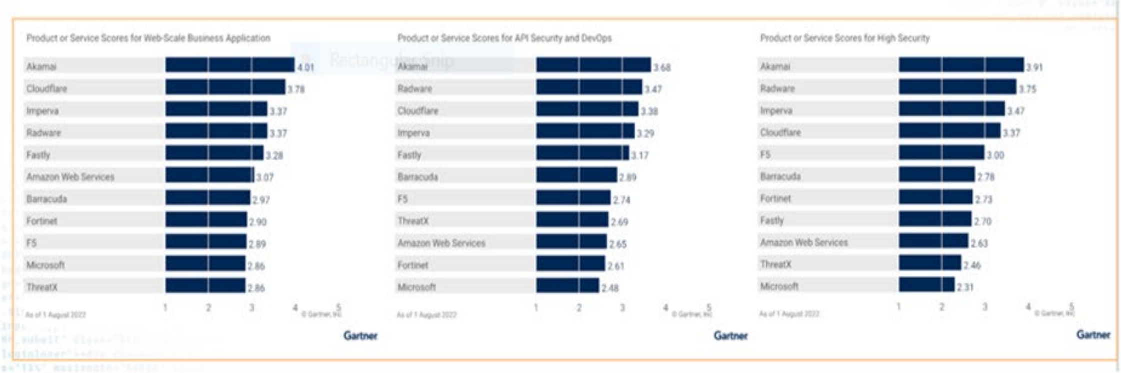
Akamai named a Leader with the highest ratings for capabilities, strategy, and market presence.

*“Akamai's balanced and comprehensive portfolio spanning media and web delivery, emerging edge applications, extensive security capabilities, and programmable edge addresses the needs of all enterprise segments and the developer community.”*

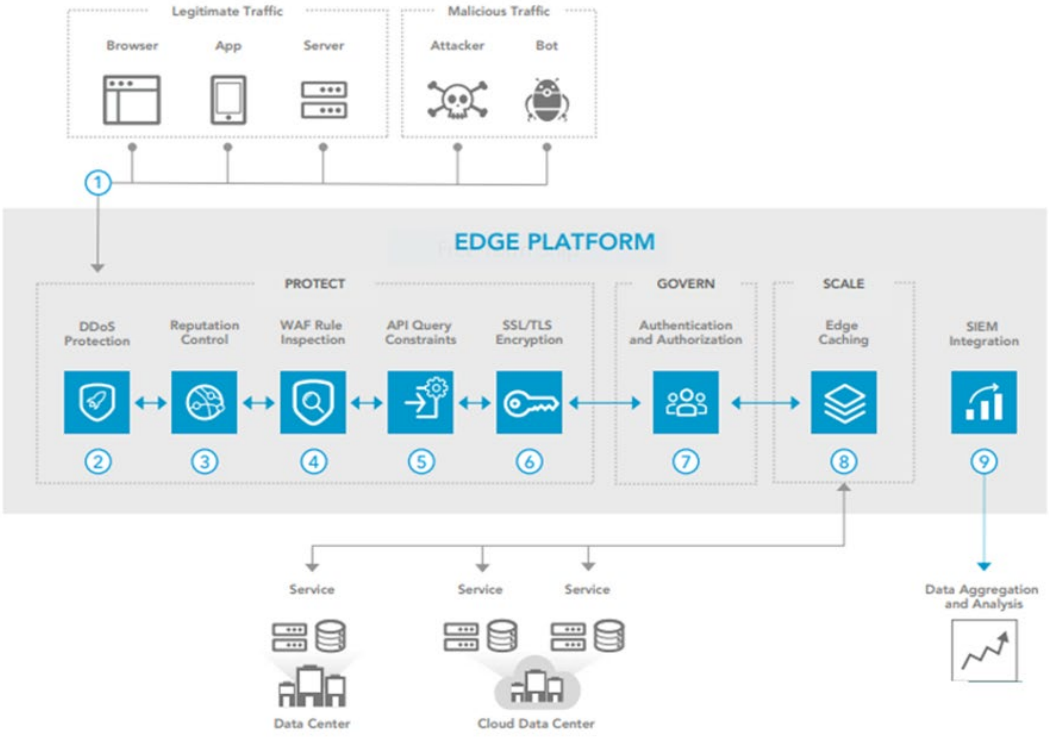


Akamai named customers' choice in **2022 Gartner® Peer Insights™ 'Voice of the Customer': Global CDN**

Akamai named customers' choice in **2023 Gartner® Peer Insights™ 'Voice of the Customer' for Cloud Web Application and API Protection**



## Example Reference Architecture by "Customer"



### 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:

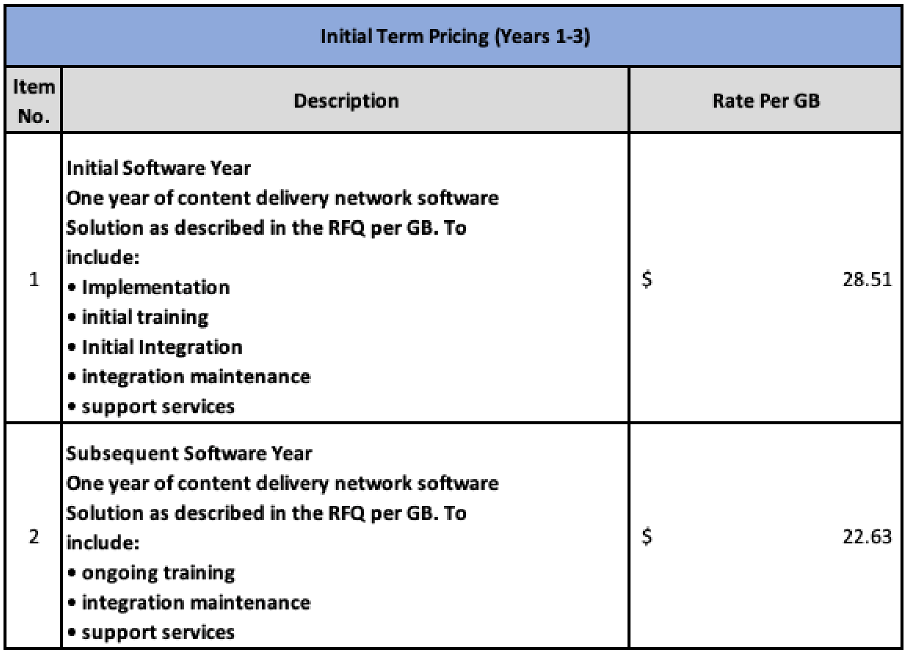
_______ 43210000-US-16-ACS Technology Products, Services, Solutions, and Related Products and Services
___X__ 43230000-NASPO-16-ACS Cloud Solutions
_______ 43230000-23-NASPO-ACS Software Value Added Reseller (SVAR)

### II. Pricing Instructions

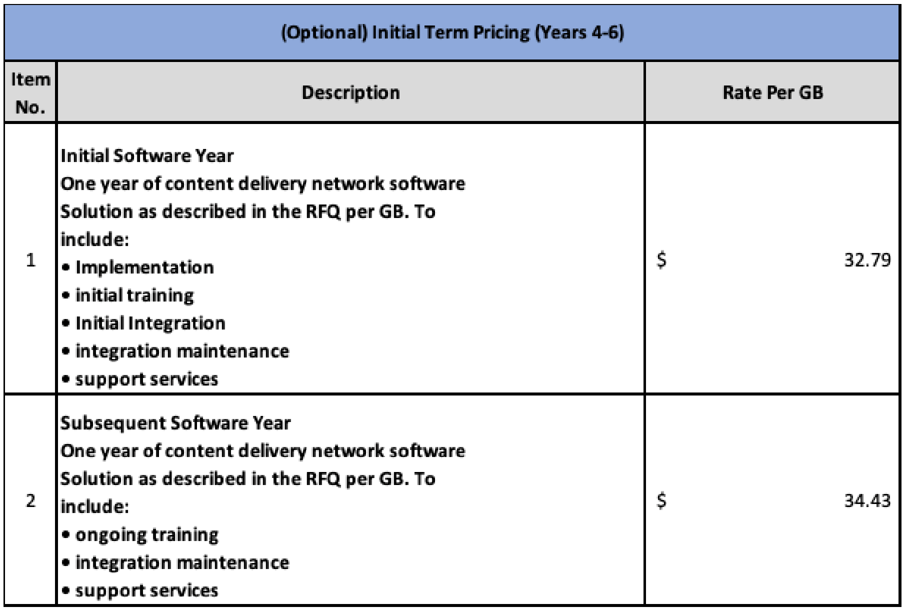
The vendor shall provide fixed rates quoted at or below the rates in the applicable ACS contract selected in Section I above. FL[DS] anticipates purchasing the external-facing asset discovery Solution for FL[DS] and all Customers. The estimated quantities listed are given only as a guideline for preparing 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

The Pricing below represents not-to-exceed (NTE) pricing. Actual pricing will be supplied once the number of customer entities and estimated traffic is confirmed.



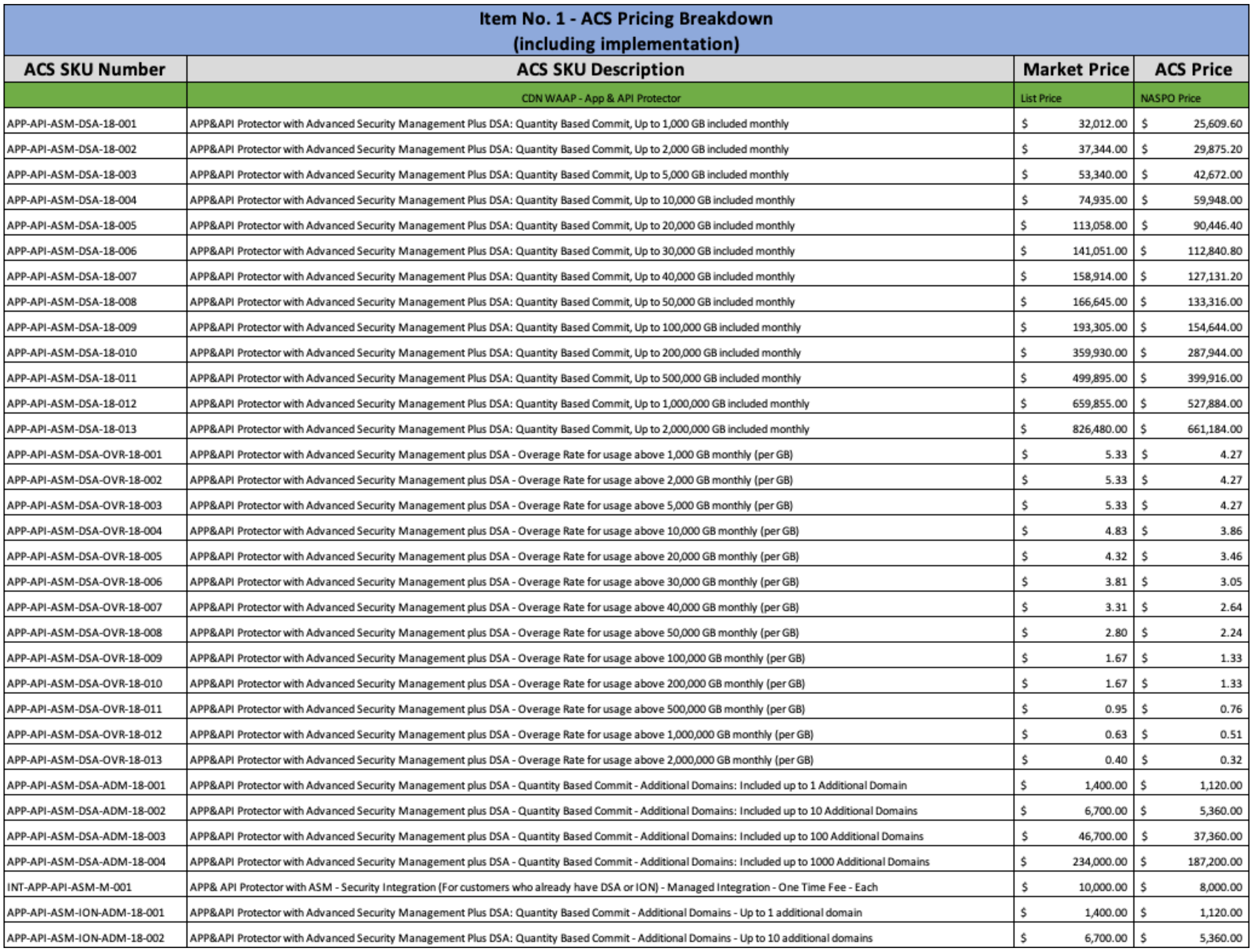
| Initial Term Pricing (Years 1-3) | | |
|---|---|---|
| Item No. | Description | Rate Per GB |
| 1 | Initial Software Year<br>One year of content delivery network software Solution as described in the RFQ per GB. To include:<br>• Implementation<br>• initial training<br>• Initial Integration<br>• integration maintenance<br>• support services | $ 28.51 |
| 2 | Subsequent Software Year<br>One year of content delivery network software Solution as described in the RFQ per GB. To include:<br>• ongoing training<br>• integration maintenance<br>• support services | $ 22.63 |



| (Optional) Initial Term Pricing (Years 4-6) | | |
|---|---|---|
| Item No. | Description | Rate Per GB |
| 1 | Initial Software Year<br>One year of content delivery network software Solution as described in the RFQ per GB. To include:<br>• Implementation<br>• initial training<br>• Initial Integration<br>• integration maintenance<br>• support services | $ 32.79 |
| 2 | Subsequent Software Year<br>One year of content delivery network software Solution as described in the RFQ per GB. To include:<br>• ongoing training<br>• integration maintenance<br>• support services | $ 34.43 |

## 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 |
|---|---|---|---|
| | CDN WAAP - App & API Protector | List Price | NASPO Price |
| APP-API-ASM-DSA-18-001 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 1,000 GB included monthly | $ 32,012.00 | $ 25,609.60 |
| APP-API-ASM-DSA-18-002 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 2,000 GB included monthly | $ 37,344.00 | $ 29,875.20 |
| APP-API-ASM-DSA-18-003 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 5,000 GB included monthly | $ 53,340.00 | $ 42,672.00 |
| APP-API-ASM-DSA-18-004 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 10,000 GB included monthly | $ 74,935.00 | $ 59,948.00 |
| APP-API-ASM-DSA-18-005 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 20,000 GB included monthly | $ 113,058.00 | $ 90,446.40 |
| APP-API-ASM-DSA-18-006 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 30,000 GB included monthly | $ 141,051.00 | $ 112,840.80 |
| APP-API-ASM-DSA-18-007 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 40,000 GB included monthly | $ 158,914.00 | $ 127,131.20 |
| APP-API-ASM-DSA-18-008 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 50,000 GB included monthly | $ 166,645.00 | $ 133,316.00 |
| APP-API-ASM-DSA-18-009 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 100,000 GB included monthly | $ 193,305.00 | $ 154,644.00 |
| APP-API-ASM-DSA-18-010 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 200,000 GB included monthly | $ 359,930.00 | $ 287,944.00 |
| APP-API-ASM-DSA-18-011 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 500,000 GB included monthly | $ 499,895.00 | $ 399,916.00 |
| APP-API-ASM-DSA-18-012 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 1,000,000 GB included monthly | $ 659,855.00 | $ 527,884.00 |
| APP-API-ASM-DSA-18-013 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 2,000,000 GB included monthly | $ 826,480.00 | $ 661,184.00 |
| APP-API-ASM-DSA-OVR-18-001 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 1,000 GB monthly (per GB) | $ 5.33 | $ 4.27 |
| APP-API-ASM-DSA-OVR-18-002 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 2,000 GB monthly (per GB) | $ 5.33 | $ 4.27 |
| APP-API-ASM-DSA-OVR-18-003 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 5,000 GB monthly (per GB) | $ 5.33 | $ 4.27 |
| APP-API-ASM-DSA-OVR-18-004 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 10,000 GB monthly (per GB) | $ 4.83 | $ 3.86 |
| APP-API-ASM-DSA-OVR-18-005 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 20,000 GB monthly (per GB) | $ 4.32 | $ 3.46 |
| APP-API-ASM-DSA-OVR-18-006 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 30,000 GB monthly (per GB) | $ 3.81 | $ 3.05 |
| APP-API-ASM-DSA-OVR-18-007 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 40,000 GB monthly (per GB) | $ 3.31 | $ 2.64 |
| APP-API-ASM-DSA-OVR-18-008 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 50,000 GB monthly (per GB) | $ 2.80 | $ 2.24 |
| APP-API-ASM-DSA-OVR-18-009 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 100,000 GB monthly (per GB) | $ 1.67 | $ 1.33 |
| APP-API-ASM-DSA-OVR-18-010 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 200,000 GB monthly (per GB) | $ 1.67 | $ 1.33 |
| APP-API-ASM-DSA-OVR-18-011 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 500,000 GB monthly (per GB) | $ 0.95 | $ 0.76 |
| APP-API-ASM-DSA-OVR-18-012 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 1,000,000 GB monthly (per GB) | $ 0.63 | $ 0.51 |
| APP-API-ASM-DSA-OVR-18-013 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 2,000,000 GB monthly (per GB) | $ 0.40 | $ 0.32 |
| APP-API-ASM-DSA-ADM-18-001 | APP&API Protector with Advanced Security Management plus DSA - Quantity Based Commit - Additional Domains: Included up to 1 Additional Domain | $ 1,400.00 | $ 1,120.00 |
| APP-API-ASM-DSA-ADM-18-002 | APP&API Protector with Advanced Security Management plus DSA - Quantity Based Commit - Additional Domains: Included up to 10 Additional Domains | $ 6,700.00 | $ 5,360.00 |
| APP-API-ASM-DSA-ADM-18-003 | APP&API Protector with Advanced Security Management plus DSA - Quantity Based Commit - Additional Domains: Included up to 100 Additional Domains | $ 46,700.00 | $ 37,360.00 |
| APP-API-ASM-DSA-ADM-18-004 | APP&API Protector with Advanced Security Management plus DSA - Quantity Based Commit - Additional Domains: Included up to 1000 Additional Domains | $ 234,000.00 | $ 187,200.00 |
| INT-APP-API-ASM-M-001 | APP& API Protector with ASM - Security Integration (For customers who already have DSA or ION) - Managed Integration - One Time Fee - Each | $ 10,000.00 | $ 8,000.00 |
| APP-API-ASM-ION-ADM-18-001 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit - Additional Domains - Up to 1 additional domain | $ 1,400.00 | $ 1,120.00 |
| APP-API-ASM-ION-ADM-18-002 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit - Additional Domains - Up to 10 additional domains | $ 6,700.00 | $ 5,360.00 |

| | | | |
|---|---|---|---|
| APP-API-ASM-DSA-ADM-18-004 | APP&API Protector with Advanced Security Management plus DSA - Quantity Based Commit - Additional Domains: Included up to 1000 Additional Domains | $ 234,000.00 | $ 187,200.00 |
| INT-APP-API-ASM-M-001 | APP& API Protector with ASM - Security Integration (For customers who already have DSA or ION) - Managed Integration - One Time Fee - Each | $ 10,000.00 | $ 8,000.00 |
| APP-API-ASM-ION-ADM-18-001 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit - Additional Domains - Up to 1 additional domain | $ 1,400.00 | $ 1,120.00 |
| APP-API-ASM-ION-ADM-18-002 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit - Additional Domains - Up to 10 additional domains | $ 6,700.00 | $ 5,360.00 |
| APP-API-ASM-ION-ADM-18-003 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit - Additional Domains - Up to 100 additional domains | $ 46,700.00 | $ 37,360.00 |
| APP-API-ASM-ION-ADM-18-004 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit - Additional Domains - Up to 1000 additional domains | $ 234,000.00 | $ 187,200.00 |
| | Akamai Secure Internet Access - ETP | | |
| ETP-000-USU-17-002 | Enterprise Threat Protector - Intelligence: Users 401-1,000 | $ 3.00 | $ 2.42 |
| ETP-000-USU-17-003 | Enterprise Threat Protector - Intelligence: Users 1,001-3,000 | $ 2.25 | $ 1.82 |
| ETP-000-USU-17-004 | Enterprise Threat Protector - Intelligence: Users 3,001-5,000 | $ 1.90 | $ 1.53 |
| ETP-000-USU-17-005 | Enterprise Threat Protector - Intelligence: Users 5,001-10,000 | $ 1.60 | $ 1.29 |
| ETP-000-USU-17-006 | Enterprise Threat Protector - Intelligence: Users 10,001-20,000 | $ 1.40 | $ 1.13 |
| ETP-000-USU-17-007 | Enterprise Threat Protector - Intelligence: Users > 20,001 | $ 1.10 | $ 0.89 |
| ETC-MIT-EAY-20-001 | Enterprise Threat Protector - Advanced Threat: Managed Integration, One Time | $ 7,093.20 | $ 7,022.26 |
| | Akamai Edge DNS | | |
| FDS-000-FDN-15-001 | Fast DNS - Standalone - Base Plan: 3 Zone Plan | $ 750.00 | $ 605.25 |
| FDS-000-FDN-15-002 | Fast DNS - Standalone - Base Plan: 10 Zone Plan | $ 1,500.00 | $ 1,210.50 |
| FDS-000-FDN-15-003 | Fast DNS - Standalone - Base Plan: 50 Zone Plan | $ 3,750.00 | $ 3,026.25 |
| FDS-000-FDN-15-004 | Fast DNS - Standalone - Base Plan: 100 Zone Plan | $ 5,250.00 | $ 4,236.75 |
| | Professional Services | | |
| SOB-000-PEF-20-001 | SOA 2.0: Base Fee, Monthly | $ 4,000.00 | $ 3,200.00 |
| SOB-000-HOC-20-001 | SOA 2.0: PS Hours (Additional Hours), Monthly Fee for Quarterly Hours, 1 - 999,999,999 | $ 117.00 | $ 93.60 |
| SOB-000-HOA-20-002 | SOA 2.0: PS Hours, Overage, As Incurred Quarterly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| SOB-000-REC-20-001 | SOA 2.0: Security Reviews (Additional Reviews), Monthly, 1 - 999,999,999 | $ 500.00 | $ 400.00 |
| SOB-ESO-PEF-20-001 | SOA 2.0: Enterprise Security Coverage, Base Fee, Monthly | $ 2,400.00 | $ 1,920.00 |
| SOB-ESO-REC-20-001 | SOA 2.0: Enterprise Security Coverage, Reviews, Monthly, 1 - 999,999,999 | $ 500.00 | $ 400.00 |
| SOB-ESO-HOC-20-001 | SOA 2.0: Enterprise Security Coverage, Hours, Quarterly, 1 - 999,999,999 | $ 117.00 | $ 93.60 |
| SOB-ESO-HOI-20-002 | SOA 2.0: Enterprise Security Coverage, Hours, Overage, As Incurred Quarterly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| SOA-AHC-15-001 | Security Optimization Assistance: Hours per Quarter, Monthly | $ 120.00 | $ 96.73 |
| SOA-AHO-15-001 | Security Optimization Assistance: Hours Overage, Quarterly | $ 350.00 | $ 282.12 |
| SOA-AR-15-001 | Security Optimization Assistance: Reviews per Year, Monthly | $ 600.00 | $ 483.63 |
| SOA-SBM-ADH-15-001 | Security Optimization Assistance for Bot Manager - Hours per Quarter | $ 120.00 | $ 96.84 |
| SOA-SBM-ADR-15-001 | Security Optimization Assistance for Bot Manager - Additional Reviews per Year | $ 600.00 | $ 484.20 |
| SOA-SBM-SOA-15-001 | Security Optimization Assistance for Bot Manager | $ 4,500.00 | $ 3,631.50 |
| SOA-SKS-ADH-15-001 | Security Optimization Assistance for Kona Site Defender - Hours per Quarter | $ 120.00 | $ 96.84 |
| SOA-SKS-ADR-15-001 | Security Optimization Assistance for Kona Site Defender - Additional Reviews per Year | $ 600.00 | $ 484.20 |
| SOA-SKS-SOD-15-001 | Security Optimization Assistance for Kona Site Defender | $ 4,500.00 | $ 3,631.50 |
| SOA-SOABM-15-001 | Security Optimization Assistance for Bot Manager: Base Fee, Monthly | $ 4,500.00 | $ 3,627.20 |
| SOA-SOAPR-15-001 | Security Optimization Assistance for Prolexic Routed: Base Fee, Monthly | $ 1,700.00 | $ 1,370.28 |
| SOA-SOAWA-15-001 | Security Optimization Assistance for Web Application Firewall: Base Fee, Monthly | $ 2,500.00 | $ 2,015.11 |
| SOA-SWP-AHI-17-001 | Security Optimization Assistance for Web Application Protector - Hours per Quarter | $ 120.00 | $ 96.84 |
| SOA-SWP-ARI-17-001 | Security Optimization Assistance for Web Application Protector - Additional Reviews per Year | $ 600.00 | $ 484.20 |
| SOA-SWP-SOA-17-001 | Security Optimization Assistance for Web Application Protector | $ 1,600.00 | $ 1,291.20 |
| SPS-000-COC-18-001 | SOA plus Service Management: Configurations | $ 600.00 | $ 484.20 |
| SPS-000-FEB-18-001 | SOA plus Service Management: Base Fee | $ 6,750.00 | $ 5,447.25 |
| SPS-000-REC-18-001 | SOA plus Service Management: Reviews | $ 600.00 | $ 484.20 |
| SPS-SRM-HOB-18-001 | SOA plus Service Management: PS Hours (Additional) | $ 108.00 | $ 87.16 |
| MINT-APP-API-ADD-P-18-001 | APP&API Protector - Security Integration - Per Additional Policy - Managed Integration - One Time Fee (For One Policy) Each | $ 3,600.00 | $ 2,880.00 |
| PPD-000-PEF-20-001 | Protect & Perform SOA with Plus: Base Fee, Monthly | $ 6,300.00 | $ 5,040.00 |
| PPD-000-SHC-20-001 | Protect & Perform SOA with Plus: PS Hours (Additional Hours), Monthly Fee for Quarterly Hours, 1 - 999,999,999 | $ 108.00 | $ 86.40 |
| PPD-000-SHI-20-002 | Protect & Perform SOA with Plus: PS Hours, Overage, As Incurred Quarterly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| PPD-PPW-COC-20-001 | Protect & Perform SOA with Plus: Health Check Configurations (Additional Configs per Check), Monthly, 1 - 10 | $ 360.00 | $ 288.00 |
| PPD-PPT-REC-20-001 | Protect & Perform SOA with Plus: Security Reviews (Additional Reviews), Monthly, 1 - 999,999,999 | $ 450.00 | $ 360.00 |
| PPD-PPQ-PEF-20-001 | Protect & Perform SOA with Plus: Enterprise Security Coverage, Base Fee, Monthly | $ 2,160.00 | $ 1,728.00 |
| PPD-PPQ-REC-20-001 | Protect & Perform SOA with Plus: Enterprise Security Coverage, Review, Monthly, 1 - 999,999,999 | $ 450.00 | $ 360.00 |
| PPD-PPQ-HOC-20-001 | Protect & Perform SOA with Plus: Enterprise Security Coverage, Hours, Commitment, Monthly, 1 - 999,999,999 | $ 117.00 | $ 93.60 |
| PPD-PPQ-HOI-20-002 | Protect & Perform SOA with Plus: Enterprise Security Coverage, Hours, Overage, Monthly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| PPF-000-PEF-20-001 | Protect & Perform SOA with Advanced: Base Fee, Monthly | $ 14,400.00 | $ 11,520.00 |
| PPF-000-SHC-20-001 | Protect & Perform SOA with Advanced: PS Hours (Additional Hours), Monthly Fee for Quarterly Hours, 1 - 999,999,999 | $ 108.00 | $ 86.40 |
| PPF-000-SHI-20-002 | Protect & Perform SOA with Advanced: PS Hours, Overage, As Incurred Quarterly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| PPF-PPO-COC-20-001 | Protect & Perform SOA with Advanced: Health Check Configurations (Additional Configs per Check), Monthly, 1 - 10 | $ 360.00 | $ 288.00 |
| PPF-PPO-TEC-20-001 | Protect & Perform SOA with Advanced: Technical Advisory Hours (Additional Hours), Monthly Fee for Quarterly Hours, 1 - 48 | $ 117.00 | $ 93.60 |
| PPF-PPO-TEI-20-002 | Protect & Perform SOA with Advanced: Technical Advisory Hours, Overage, As Incurred Quarterly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| PPF-PPT-REC-20-001 | Protect & Perform SOA with Advanced: Security Reviews (Additional Reviews), Monthly, 1 - 999,999,999 | $ 450.00 | $ 360.00 |
| PPF-PPQ-PEF-20-001 | Protect & Perform SOA with Advanced: Enterprise Security Coverage, Base Fee, Monthly | $ 2,160.00 | $ 1,728.00 |

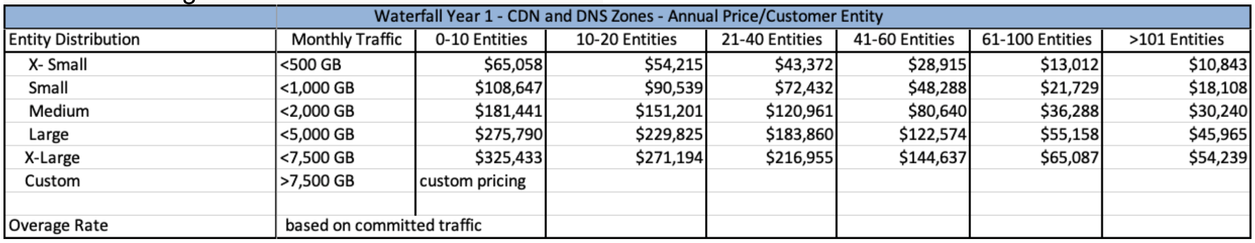
| | | | |
|---|---|---|---|
| PPF-APM-PEF-19-001 | Protect & Perform SOA with Advanced: Advanced Project Mgmt Option, Base Fee, Monthly | $ 3,150.00 | $ 2,520.00 |
| PPF-PPQ-REC-20-001 | Protect & Perform SOA with Advanced: Enterprise Security Coverage, Review, Monthly, 1 - 999,999,999 | $ 450.00 | $ 360.00 |
| PPF-PPQ-HOC-20-001 | Protect & Perform SOA with Advanced: Enterprise Security Coverage, Hours, Commitment, Monthly, 1 - 999,999,999 | $ 117.00 | $ 93.60 |
| PPF-PPQ-HOI-20-002 | Protect & Perform SOA with Advanced: Enterprise Security Coverage, Hours, Overage, Monthly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| PPF-APM-HOC-20-001 | Protect & Perform SOA with Advanced: Advanced Project Mgmt Option, Hours, Commitment, Monthly, 1 - 48 | $ 100.00 | $ 80.00 |
| PPF-APM-HOI-20-002 | Protect & Perform SOA with Advanced: Advanced Project Mgmt Option, Hours, Overage, Monthly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| PPE-000-PEF-20-001 | Protect & Perform SOA with Premium: Base Fee, Monthly | $ 30,600.00 | $ 24,480.00 |
| PPE-000-SHC-20-001 | Protect & Perform SOA with Premium: PS Hours (Additional Hours), Monthly Fee for Quarterly Hours, 1 - 999,999,999 | $ 108.00 | $ 86.40 |
| PPE-000-SHI-20-002 | Protect & Perform SOA with Premium: PS Hours, Overage, As Incurred Quarterly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| PPE-PPN-PRC-20-001 | Protect & Perform SOA with Premium: Proactive Monitoring Configurations (Additional Configs per Check), Monthly, 1 - 999,999,999 | $ 360.00 | $ 288.00 |
| PPE-PPN-TEC-20-001 | Protect & Perform SOA with Premium: Technical Advisory Hours (Additional Hours), Monthly Fee for Quarterly Hours, 1 - 999,999,999 | $ 117.00 | $ 93.60 |
| PPE-PPN-TEI-20-002 | Protect & Perform SOA with Premium: Technical Advisory Hours, Overage, As Incurred Quarterly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| PPE-PPN-SUC-20-001 | Protect & Perform SOA with Premium: Support Advocacy Hours (Additional Hours), Monthly Fee for Quarterly Hours, 1 - 999,999,999 | $ 100.00 | $ 80.00 |
| PPE-PPT-REC-20-001 | Protect & Perform SOA with Premium: Security Reviews (Additional Reviews), Monthly, 1 - 999,999,999 | $ 450.00 | $ 360.00 |
| PPE-PPN-ASC-20-001 | Protect & Perform SOA with Premium: Business Assessments (Additional Assessments), Monthly, 1 - 12 | $ 675.00 | $ 540.00 |
| PPE-PPQ-PEF-20-001 | Protect & Perform SOA with Premium: Enterprise Security Coverage, Base Fee, Monthly | $ 2,160.00 | $ 1,728.00 |
| PPE-PPQ-REC-20-001 | Protect & Perform SOA with Premium: Enterprise Security Coverage, Reviews, Monthly, 1 - 999,999,999 | $ 450.00 | $ 360.00 |
| PPE-PPQ-HOC-20-001 | Protect & Perform SOA with Premium: Enterprise Security Coverage, Hours, Quarterly, 1 - 999,999,999 | $ 117.00 | $ 93.60 |
| PPE-PPQ-HOI-20-002 | Protect & Perform SOA with Premium: Enterprise Security Coverage, Hours, Overage, As Incurred Quarterly, 1 - 999,999,999 | $ 350.00 | $ 280.00 |
| PPE-ATS-PEC-19-001 | Protect & Perform SOA with Premium: Additional Technical Support Alignment, Monthly | $ 7,200.00 | $ 5,760.00 |
| PSE-000-PSH-15-001 | PS Enterprise hours | $ 350.00 | $ 282.45 |
| | Professional Services | | |
| PS-AP | Professional Services- Application Programmer - Per Hour | $ 250.00 | $ 242.95 |
| PS-BA | Professional Services - Business Analyst - Per Hour | $ 250.00 | $ 242.95 |
| PS-BSA | Professional Services - Business Systems Analyst - Per Hour | $ 350.00 | $ 340.13 |
| PS-BSMS | Professional Services - Business Subject Matter Specialist - Per Hour | $ 350.00 | $ 340.13 |
| PS-CES | Professional Services - Contractor, Enterprise Solutions - Per Hour | $ 250.00 | $ 242.95 |
| PS-CSDM | Professional Services - Client/Server Database Manager - Per Hour | $ 300.00 | $ 291.54 |
| PS-CSNA | Professional Services - Client/Server Network Architect - Per Hour | $ 400.00 | $ 388.72 |
| PS-DA | Professional Services - Data Architect - Per Hour | $ 300.00 | $ 291.54 |
| PS-DSA | Professional Services - Data Security Analyst - Per Hour | $ 225.00 | $ 218.66 |
| PS-ENG | Professional Services - Software Engineering 5 Day Bundle | $ 20,000.00 | $ 19,436.00 |
| PS-ERP | Professional Services - ERP Analyst - Per Hour | $ 450.00 | $ 437.31 |
| PS-GS | Professional Services - Graphic Specialist - Per Hour | $ 200.00 | $ 194.36 |
| PS-NE | Professional Services - Network Engineer - Per Hour | $ 350.00 | $ 340.13 |
| PS-SAP | Professional Services - Senior App. Programmer - Per Hour | $ 275.00 | $ 267.25 |
| PS-SBA | Professional Services - Senior Business Analyst - Per Hour | $ 275.00 | $ 267.25 |
| PS-SCES | Professional Services - Senior Contractor, Enterprise Solutions - Per Hour | $ 300.00 | $ 291.54 |
| PS-SDSA | Professional Services - Senior Data Security Analyst - Per Hour | $ 275.00 | $ 267.25 |
| PS-SGS | Professional Services - Senior Graphic Specialist - Per Hour | $ 250.00 | $ 242.95 |
| PS-SIAE | Professional Services - Senior Information Assurance Engineer - Per Hour | $ 400.00 | $ 388.72 |
| PS-SNE | Professional Services - Senior Network Engineer - Per Hour | $ 400.00 | $ 388.72 |
| PS-SPA | Professional Services - Senior Principle Advisor - Per Hour | $ 500.00 | $ 485.90 |
| PS-SSE | Professional Services - Senior Software Engineer - Per Hour | $ 275.00 | $ 267.25 |
| PS-STPM | Professional Services - Senior Technical Project Manager - Per Hour | $ 375.00 | $ 364.43 |
| PS-SUPP-1 | Services to support Customer Implementation - Requires SOW (up to 12 months) | $ 25,000.00 | $ 24,295.00 |
| PS-TPM | Professional Services - Technical Project Manager - Per Hour | $ 300.00 | $ 291.54 |
| PS-CUSTI-1 | Customer Implementation Services - Requires SOW (up to 30 days) | $ 100,000.00 | $ 97,180.00 |

| Item No. 2 – ACS Pricing Breakdown<br>(without implementation) | | | |
|---|---|---|---|
| **ACS SKU Number** | **ACS SKU Description** | **Market Price** | **ACS Price** |
| | CDN WAAP - App & API Protector | List Price | NASPO Price |
| APP-API-ASM-DSA-18-001 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 1,000 GB included monthly | $ 32,012.00 | $ 25,609.60 |
| APP-API-ASM-DSA-18-002 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 2,000 GB included monthly | $ 37,344.00 | $ 29,875.20 |
| APP-API-ASM-DSA-18-003 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 5,000 GB included monthly | $ 53,340.00 | $ 42,672.00 |
| APP-API-ASM-DSA-18-004 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 10,000 GB included monthly | $ 74,935.00 | $ 59,948.00 |
| APP-API-ASM-DSA-18-005 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 20,000 GB included monthly | $ 113,058.00 | $ 90,446.40 |
| APP-API-ASM-DSA-18-006 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 30,000 GB included monthly | $ 141,051.00 | $ 112,840.80 |
| APP-API-ASM-DSA-18-007 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 40,000 GB included monthly | $ 158,914.00 | $ 127,131.20 |
| APP-API-ASM-DSA-18-008 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 50,000 GB included monthly | $ 166,645.00 | $ 133,316.00 |
| APP-API-ASM-DSA-18-009 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 100,000 GB included monthly | $ 193,305.00 | $ 154,644.00 |
| APP-API-ASM-DSA-18-010 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 200,000 GB included monthly | $ 359,930.00 | $ 287,944.00 |
| APP-API-ASM-DSA-18-011 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 500,000 GB included monthly | $ 499,895.00 | $ 399,916.00 |
| APP-API-ASM-DSA-18-012 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 1,000,000 GB included monthly | $ 659,855.00 | $ 527,884.00 |
| APP-API-ASM-DSA-18-013 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit, Up to 2,000,000 GB included monthly | $ 826,480.00 | $ 661,184.00 |
| APP-API-ASM-DSA-OVR-18-001 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 1,000 GB monthly (per GB) | $ 5.33 | $ 4.27 |
| APP-API-ASM-DSA-OVR-18-002 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 2,000 GB monthly (per GB) | $ 5.33 | $ 4.27 |
| APP-API-ASM-DSA-OVR-18-003 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 5,000 GB monthly (per GB) | $ 5.33 | $ 4.27 |
| APP-API-ASM-DSA-OVR-18-004 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 10,000 GB monthly (per GB) | $ 4.83 | $ 3.86 |
| APP-API-ASM-DSA-OVR-18-005 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 20,000 GB monthly (per GB) | $ 4.32 | $ 3.46 |
| APP-API-ASM-DSA-OVR-18-006 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 30,000 GB monthly (per GB) | $ 3.81 | $ 3.05 |
| APP-API-ASM-DSA-OVR-18-007 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 40,000 GB monthly (per GB) | $ 3.31 | $ 2.64 |
| APP-API-ASM-DSA-OVR-18-008 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 50,000 GB monthly (per GB) | $ 2.80 | $ 2.24 |
| APP-API-ASM-DSA-OVR-18-009 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 100,000 GB monthly (per GB) | $ 1.67 | $ 1.33 |
| APP-API-ASM-DSA-OVR-18-010 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 200,000 GB monthly (per GB) | $ 1.67 | $ 1.33 |
| APP-API-ASM-DSA-OVR-18-011 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 500,000 GB monthly (per GB) | $ 0.95 | $ 0.76 |
| APP-API-ASM-DSA-OVR-18-012 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 1,000,000 GB monthly (per GB) | $ 0.63 | $ 0.51 |
| APP-API-ASM-DSA-OVR-18-013 | APP&API Protector with Advanced Security Management plus DSA - Overage Rate for usage above 2,000,000 GB monthly (per GB) | $ 0.40 | $ 0.32 |
| APP-API-ASM-DSA-ADM-18-001 | APP&API Protector with Advanced Security Management plus DSA - Quantity Based Commit - Additional Domains: Included up to 1 Additional Domain | $ 1,400.00 | $ 1,120.00 |
| APP-API-ASM-DSA-ADM-18-002 | APP&API Protector with Advanced Security Management plus DSA - Quantity Based Commit - Additional Domains: Included up to 10 Additional Domains | $ 6,700.00 | $ 5,360.00 |
| APP-API-ASM-DSA-ADM-18-003 | APP&API Protector with Advanced Security Management plus DSA - Quantity Based Commit - Additional Domains: Included up to 100 Additional Domains | $ 46,700.00 | $ 37,360.00 |
| APP-API-ASM-DSA-ADM-18-004 | APP&API Protector with Advanced Security Management plus DSA - Quantity Based Commit - Additional Domains: Included up to 1000 Additional Domains | $ 234,000.00 | $ 187,200.00 |
| INT-APP-API-ASM-M-001 | APP& API Protector with ASM - Security Integration (For customers who already have DSA or ION) - Managed Integration - One Time Fee - Each | $ 10,000.00 | $ 8,000.00 |
| APP-API-ASM-ION-ADM-18-001 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit - Additional Domains - Up to 1 additional domain | $ 1,400.00 | $ 1,120.00 |
| APP-API-ASM-ION-ADM-18-002 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit - Additional Domains - Up to 10 additional domains | $ 6,700.00 | $ 5,360.00 |
| APP-API-ASM-ION-ADM-18-003 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit - Additional Domains - Up to 100 additional domains | $ 46,700.00 | $ 37,360.00 |
| APP-API-ASM-ION-ADM-18-004 | APP&API Protector with Advanced Security Management Plus DSA: Quantity Based Commit - Additional Domains - Up to 1000 additional domains | $ 234,000.00 | $ 187,200.00 |
| | Akamai Secure Internet Access - ETP | | |
| ETP-000-USU-17-002 | Enterprise Threat Protector - Intelligence: Users 401-1,000 | $ 3.00 | $ 2.42 |
| ETP-000-USU-17-003 | Enterprise Threat Protector - Intelligence: Users 1,001-3,000 | $ 2.25 | $ 1.82 |
| ETP-000-USU-17-004 | Enterprise Threat Protector - Intelligence: Users 3,001-5,000 | $ 1.90 | $ 1.53 |
| ETP-000-USU-17-005 | Enterprise Threat Protector - Intelligence: Users 5,001-10,000 | $ 1.60 | $ 1.29 |
| ETP-000-USU-17-006 | Enterprise Threat Protector - Intelligence: Users 10,001-20,000 | $ 1.40 | $ 1.13 |
| ETP-000-USU-17-007 | Enterprise Threat Protector - Intelligence: Users > 20,001 | $ 1.10 | $ 0.89 |
| ETC-MIT-EAY-20-001 | Enterprise Threat Protector - Advanced Threat: Managed Integration, One Time | $ 7,093.20 | $ 7,022.26 |
| | Akamai Edge DNS | | |
| FDS-000-FDN-15-001 | Fast DNS - Standalone - Base Plan: 3 Zone Plan | $ 750.00 | $ 605.25 |
| FDS-000-FDN-15-002 | Fast DNS - Standalone - Base Plan: 10 Zone Plan | $ 1,500.00 | $ 1,210.50 |
| FDS-000-FDN-15-003 | Fast DNS - Standalone - Base Plan: 50 Zone Plan | $ 3,750.00 | $ 3,026.25 |
| FDS-000-FDN-15-004 | Fast DNS - Standalone - Base Plan: 100 Zone Plan | $ 5,250.00 | $ 4,236.75 |

## V. Waterfall Pricing (Optional)

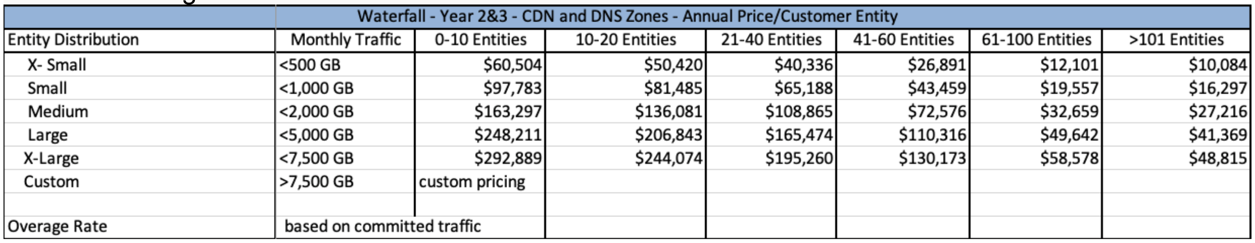
The Department is seeking an optional waterfall pricing model which leverages volume discounts. Vendors are encouraged to provide a pricing structure which specifies a volume range at which larger discounts could be applied. This alternative pricing shall be in addition to the pricing provided in Section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

Waterfall Pricing for CDN and DNS Zones – Year 1



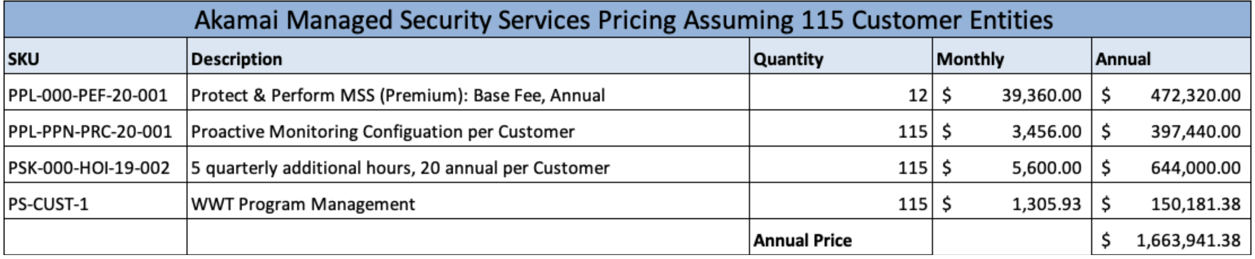
| | Waterfall Year 1 - CDN and DNS Zones - Annual Price/Customer Entity | | | | | | |
|---|---|---|---|---|---|---|---|
| Entity Distribution | Monthly Traffic | 0-10 Entities | 10-20 Entities | 21-40 Entities | 41-60 Entities | 61-100 Entities | >101 Entities |
| X- Small | <500 GB | $65,058 | $54,215 | $43,372 | $28,915 | $13,012 | $10,843 |
| Small | <1,000 GB | $108,647 | $90,539 | $72,432 | $48,288 | $21,729 | $18,108 |
| Medium | <2,000 GB | $181,441 | $151,201 | $120,961 | $80,640 | $36,288 | $30,240 |
| Large | <5,000 GB | $275,790 | $229,825 | $183,860 | $122,574 | $55,158 | $45,965 |
| X-Large | <7,500 GB | $325,433 | $271,194 | $216,955 | $144,637 | $65,087 | $54,239 |
| Custom | >7,500 GB | custom pricing | | | | | |
| | | | | | | | |
| Overage Rate | based on committed traffic | | | | | | |

Waterfall Pricing for CDN and DNS Zones – Year 2 & 3



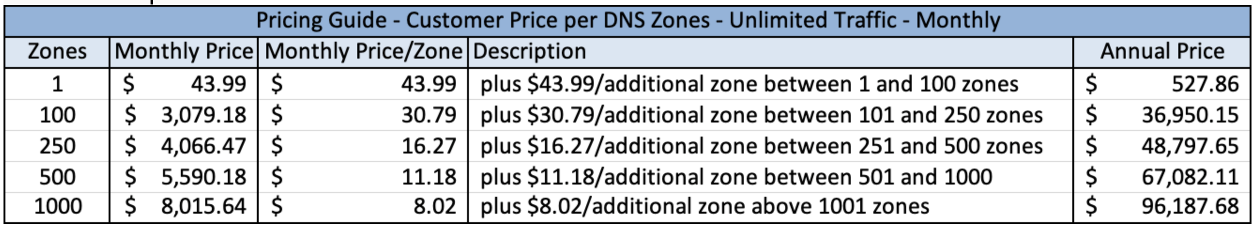
| | Waterfall - Year 2&3 - CDN and DNS Zones - Annual Price/Customer Entity | | | | | | |
|---|---|---|---|---|---|---|---|
| Entity Distribution | Monthly Traffic | 0-10 Entities | 10-20 Entities | 21-40 Entities | 41-60 Entities | 61-100 Entities | >101 Entities |
| X- Small | <500 GB | $60,504 | $50,420 | $40,336 | $26,891 | $12,101 | $10,084 |
| Small | <1,000 GB | $97,783 | $81,485 | $65,188 | $43,459 | $19,557 | $16,297 |
| Medium | <2,000 GB | $163,297 | $136,081 | $108,865 | $72,576 | $32,659 | $27,216 |
| Large | <5,000 GB | $248,211 | $206,843 | $165,474 | $110,316 | $49,642 | $41,369 |
| X-Large | <7,500 GB | $292,889 | $244,074 | $195,260 | $130,173 | $58,578 | $48,815 |
| Custom | >7,500 GB | custom pricing | | | | | |
| | | | | | | | |
| Overage Rate | based on committed traffic | | | | | | |

Managed Services (MDR)

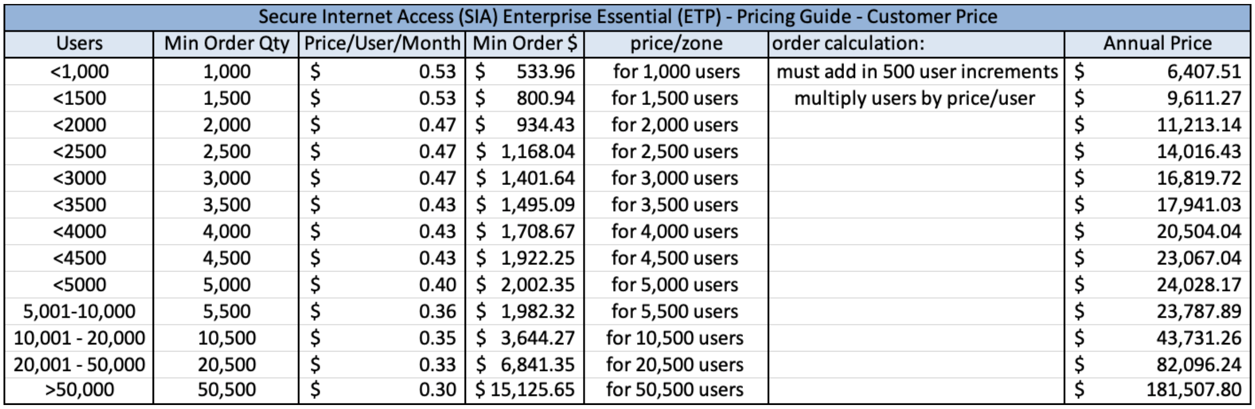


| Akamai Managed Security Services Pricing Assuming 115 Customer Entities | | | | |
|---|---|---|---|---|
| **SKU** | **Description** | **Quantity** | **Monthly** | **Annual** |
| PPL-000-PEF-20-001 | Protect & Perform MSS (Premium): Base Fee, Annual | 12 | $ 39,360.00 | $ 472,320.00 |
| PPL-PPN-PRC-20-001 | Proactive Monitoring Configuation per Customer | 115 | $ 3,456.00 | $ 397,440.00 |
| PSK-000-HOI-19-002 | 5 quarterly additional hours, 20 annual per Customer | 115 | $ 5,600.00 | $ 644,000.00 |
| PS-CUST-1 | WWT Program Management | 115 | $ 1,305.93 | $ 150,181.38 |
| | | **Annual Price** | | $ 1,663,941.38 |

Additional Options



| Pricing Guide - Customer Price per DNS Zones - Unlimited Traffic - Monthly | | | | |
|---|---|---|---|---|
| Zones | Monthly Price | Monthly Price/Zone | Description | Annual Price |
| 1 | $ 43.99 | $ 43.99 | plus $43.99/additional zone between 1 and 100 zones | $ 527.86 |
| 100 | $ 3,079.18 | $ 30.79 | plus $30.79/additional zone between 101 and 250 zones | $ 36,950.15 |
| 250 | $ 4,066.47 | $ 16.27 | plus $16.27/additional zone between 251 and 500 zones | $ 48,797.65 |
| 500 | $ 5,590.18 | $ 11.18 | plus $11.18/additional zone between 501 and 1000 | $ 67,082.11 |
| 1000 | $ 8,015.64 | $ 8.02 | plus $8.02/additional zone above 1001 zones | $ 96,187.68 |



Secure Internet Access (SIA) Enterprise Essential (ETP) - Pricing Guide - Customer Price

| Users | Min Order Qty | Price/User/Month | Min Order $ | price/zone | order calculation: | Annual Price |
|---|---|---|---|---|---|---|
| <1,000 | 1,000 | $ 0.53 | $ 533.96 | for 1,000 users | must add in 500 user increments | $ 6,407.51 |
| <1500 | 1,500 | $ 0.53 | $ 800.94 | for 1,500 users | multiply users by price/user | $ 9,611.27 |
| <2000 | 2,000 | $ 0.47 | $ 934.43 | for 2,000 users | | $ 11,213.14 |
| <2500 | 2,500 | $ 0.47 | $ 1,168.04 | for 2,500 users | | $ 14,016.43 |
| <3000 | 3,000 | $ 0.47 | $ 1,401.64 | for 3,000 users | | $ 16,819.72 |
| <3500 | 3,500 | $ 0.43 | $ 1,495.09 | for 3,500 users | | $ 17,941.03 |
| <4000 | 4,000 | $ 0.43 | $ 1,708.67 | for 4,000 users | | $ 20,504.04 |
| <4500 | 4,500 | $ 0.43 | $ 1,922.25 | for 4,500 users | | $ 23,067.04 |
| <5000 | 5,000 | $ 0.40 | $ 2,002.35 | for 5,000 users | | $ 24,028.17 |
| 5,001-10,000 | 5,500 | $ 0.36 | $ 1,982.32 | for 5,500 users | | $ 23,787.89 |
| 10,001 - 20,000 | 10,500 | $ 0.35 | $ 3,644.27 | for 10,500 users | | $ 43,731.26 |
| 20,001 - 50,000 | 20,500 | $ 0.33 | $ 6,841.35 | for 20,500 users | | $ 82,096.24 |
| >50,000 | 50,500 | $ 0.30 | $ 15,125.65 | for 50,500 users | | $ 181,507.80 |

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

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

## 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.

Value-Added Services (Free to the end user) included in this solution are as follows.

- Access to World Wide Technology’s Advance Technology Center (ATC)
    - The ATC has hundreds of labs that are free to customers.
    - You only need to sign up for your free account with your work email.
- Akamai implementation is included in the subscription service.
- Akamai University Self-Paced Video Learning through the Akamai University

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

World Wide Technology, LLC

Vendor Name

43-1912895

FEIN

May 12, 2023

Date

Signature

Gregory Brush

Signatory Printed Name

# 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 |

# 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-22/23-156, Content Delivery Network (CDN) Solution ("Solution");

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

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

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

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

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

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

(f) State: The State of Florida.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**FLORIDA DEPARTMENT**
**OF MANAGEMENT SERVICES**

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

Name: Pedro Allende

Title: Secretary

Date: 6/14/2023 | 4:59 PM EDT

**World Wide Technology, LLC**

By: Gregory Brush Digitally signed by Gregory Brush Date: 2023.05.15 13:38:38 -05'00'

Name: Gregory Brush

Title: Area Vice President, Public Sector

Date: May 15, 2023