

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

**AGENCY TERM CONTRACT
FOR
CONTENT DELIVERY NETWORK
DMS-22/23-156A
BETWEEN
STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES
AND
PRESIDIO NETWORKED SOLUTIONS LLC**

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 PRESIDIO NETWORKED SOLUTIONS LLC (Contractor), with offices at 5337 Millenia Lakes Boulevard, Suite 300, Orlando, FL 32839, 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:

Emily Phares
Account Manager
5337 Millenia Lakes Boulevard, Suite 300
Orlando, FL 32839
Telephone: (850) 270-2988
Email: ephares@presidio.com

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

9.0 Assignment

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

10.0 Price Decreases

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

11.0 Additions/Deletions

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

PRESIDIO NETWORKED SOLUTIONS LLC:

STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES:

DocuSigned by:
Erik Hayko
E7A28D0E9E4548D...
Authorized Signature

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

Erik Hayko
Print Name

6/29/2023 | 3:37 PM EDT
Date

Senior Contracts Manager
Title

6/29/2023 | 2:51 PM 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 DELIVERABLES AND FINANCIAL CONSEQUENCES			
No.	Deliverable	Time Frame	Financial Consequences
1	The Contractor shall host a kickoff meeting with the Purchaser individually, and kickoff meeting with each additional Customer, and FL[DS] (if applicable) in accordance with the PO, and any applicable ATC.	The Contractor shall host the meeting within five (5) calendar days of PO issuance.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after deliverable due date.
2	The Contractor shall submit the Implementation Plan timely and in accordance with the PO and any applicable ATC.	The Contractor shall collaborate with the Customer and submit each Customer's Implementation Plan to the Purchaser and each additional Customer within 10 calendar days of PO issuance.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after the deliverable due date until the Customer Implementation Plan is received. Financial consequences shall also be assessed for a Customer's Implementation Plan submitted that is not in accordance with the PO and any applicable ATC, in the amount of \$500 for each incomplete Implementation Plan.

**TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES**

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

**TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES**

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

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

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

8.0 PERFORMANCE MEASURES

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

8.1 Performance Compliance

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

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

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

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

9.0 FINANCIAL CONSEQUENCES

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

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

10.0 **RESPONSE CONTENT AND FORMAT**

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

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

- 1) Documentation to describe the 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 Registration Link: https://us02web.zoom.us/meeting/register/tZEIcEqvqz0tHtJ5CTHAPP5dXloquUoX0FZw	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 IDENTIFICATION AND PROTECTION OF CONFIDENTIAL INFORMATION

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

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

legal action to assert that the information in question is exempt from disclosure under Chapter 119, F.S., or other applicable law.

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

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

22.0 USE OF SUBCONTRACTORS

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

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

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

23.0 LEGISLATIVE APPROPRIATION

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

24.0 MODIFICATIONS

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

25.0 CONFLICT OF INTEREST

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

26.0 DISCRIMINATORY, CONVICTED AND ANTITRUST VENDORS LISTS

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

27.0 E-VERIFY

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

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

28.0 COOPERATION WITH INSPECTOR GENERAL

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

29.0 ACCESSIBILITY

The Contractor will comply with section 508 of the Rehabilitation Act of 1973, as amended and 29 U.S.C. s. 794(d), including the regulations set forth under 36 C.F.R. part 1194. Section 282.601(1), F.S., states that "state government shall, when developing, competitively procuring, maintaining, or using electronic information or information technology acquired on

or after July 1, 2006, ensure that State employees with disabilities have access to and are provided with information and data comparable to the access and use by State employees who are not individuals with disabilities.”

30.0 PRODUCTION AND INSPECTION

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

31.0 SCRUTINIZED COMPANIES

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

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

32.0 BACKGROUND SCREENING

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

32.1 Background Check

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

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

“Data” means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions, whether it is exempt, confidential, or

personal health information. Data may be in any form, including but not limited to, storage media, computer memory, in transit, presented on a display device, or in physical media such as paper, film, microfilm, or microfiche. Data includes the original form of the Data and all metadata associated with the Data.

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

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

32.2 Disqualifying Offenses

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

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

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

32.3 Refresh Screening

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

32.4 Self-Disclosure

The Contractor shall ensure that all Persons have a responsibility to self-report within three calendar days to the Contractor any updated court disposition regarding any disqualifying offense, regardless of adjudication (adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict). The Contractor shall immediately reassess

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

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

32.5 Duty to Provide Security Data

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

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

32.6 Screening Compliance Audits and Security Inspections

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

32.7 Record Retention

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

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

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

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

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

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

32.8 Indemnification

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

33.0 LOCATION OF DATA

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

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

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

34.0 DATA TRANSMISSION

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

35.0 TERMS AND CONDITIONS

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

36.0 COOPERATIVE PURCHASING

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

37.0 PRICE ADJUSTMENTS

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

38.0 FINANCIAL STABILITY

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

39.0 RFQ ATTACHMENTS

Attachment A, Price Sheet

Attachment B, Contact Information Sheet

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

Department's Purchase Order Terms and Conditions

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

**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	<p><u>Initial Software Year</u> One year of content delivery network software Solution as described in the RFQ per gigabyte (GB). To include:</p> <ul style="list-style-type: none"> • Implementation • initial training • Initial Integration • integration maintenance • support services 	\$ _____
2	<p><u>Subsequent Software Year</u> One year of content delivery network software Solution as described in the RFQ per GB. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ _____

Optional Renewal Term Pricing (Years 4-6)		
Item No.	Description	Rate Per GB
1	<u>Initial Software Year</u> One year of content delivery network software Solution as described in the RFQ per GB. To include: <ul style="list-style-type: none"> • Implementation • initial training • Initial Integration • integration maintenance • support services 	\$ _____
2	<u>Subsequent Software Year</u> One year of content delivery network software Solution as described in the RFQ per GB. To include: <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ _____

IV. ACS Price Breakdown

In the table below, the vendor shall provide the pricing breakdown to document the pricing is in accordance with the applicable ACS contract. The vendor shall provide the ACS SKU Numbers, ACS SKU Descriptions, Market Price, and ACS Price that encompass the services as described in the RFQ:

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price

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

V. Waterfall Pricing (Optional)

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

VI. State of Florida Enterprise Pricing (Optional)

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

VII. Value-Added Services (Optional)

If vendors are able to offer additional services and/or commodities for 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:		



PROPOSAL RESPONSE

Florida Digital Service Content Delivery Network (CDN) Solution

Request for Quote (RFQ): DMS-22/23-156

Submit via Cloud Solutions (43230000-NASPO-16-ACS)



TABLE OF CONTENTS

1)	CONTENT DELIVERY NETWORK (CDN) DISCOVERY SOFTWARE SOLUTION DOCUMENTATION.....	1
a)	Draft SLA	21
b)	Training & Support sla	21
c)	Implementation plan	22
d)	MDR SLA (optional).....	37
e)	Future Integrations SLA (optional)	38
f)	Disaster Recovery Plan.....	38
2)	EXPERIENCE	40
3)	IMPLEMENTATION	41
4)	VALUE-ADDED SERVICES	42
5)	ATTACHMENT A – PRICE SHEET.....	45
6)	ATTACHMENT B – CONTACT INFORMATION SHEET.....	50
7)	NON-DISCLOSURE AGREEMENT	51
	ADDENDUM I.....	52

TABLE OF EXHIBITS

No table of figures entries found.

1) CONTENT DELIVERY NETWORK (CDN) DISCOVERY SOFTWARE SOLUTION DOCUMENTATION

Presidio proposes Cloudflare to provide a content delivery network solution for FL[DS]. Below are the details of how Cloudflare meets the requirements of this RFQ.

Cloudflare's Content Delivery Network (CDN) solution is designed to improve the performance, reliability, and scalability of delivering content over the internet through its unique Anycast Network. Cloudflare's CDN aligns with the requirements mentioned, which include efficient distribution of web content to end-users across different geographical locations.

Cloudflare Network: Cloudflare's network spans across numerous data centers worldwide with over 485+ points of presence, of which 90+ reside in the U.S., strategically distributed to optimize content delivery. This global network infrastructure allows for improved performance and scalability.

Cloudflare Content Delivery: Cloudflare's content delivery features focus on caching, compression, and optimization techniques to efficiently deliver static and dynamic content. These features contribute to faster and more reliable content delivery despite what device the content is being sent to or operating system it's running.

By leveraging Cloudflare's network of over 485 geographically distributed servers, 90 of which reside in the United States, Cloudflare aims to reduce latency, enhance availability, scale bandwidth, and optimize content delivery to ensure a superior user experience for end-users accessing web content.

Cloudflare CDN: Please see Addendum I for information sheets on Cloudflare's Reference Architecture, DDoS, Web Application Firewall, Bot Management, Load Balancing, Cloud Delivered Security, Application Security Bundle, and Premium Success.

RFQ Text:

Documentation to describe the external-facing asset discovery software Solution proposed and how it meets the requirements of this RFQ.

6.0 SCOPE OF WORK

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.

Response: Cloudflare's Content Delivery Network (CDN) solution is designed and implemented to comply with cybersecurity statutes and rules, including those specific to Florida. It incorporates multiple layers of security to ensure robust protection.

Cloudflare Security Services: Cloudflare offers a range of security services that align with the mentioned requirements. These services include network and application firewalls, DDoS protection, SSL encryption, secure DNS, web application firewall (WAF), bot detection, and real-time threat detection and response mechanisms.

Cloudflare WAF: Cloudflare's Web Application Firewall (WAF) provides protection against various cyber threats, including application-layer attacks. It helps comply with security regulations by implementing rules and policies to mitigate risks.

Cloudflare WAF: Cloudflare's WAF was also Named a Leader in the Forrester Wave™: Web Application Firewalls in late 2022.

Cloudflare WAF & API Protection: Cloudflare's WAF was named a leader in Gartner's 2022 Magic Quadrant for Web Application & API Protection.

Cloudflare DDoS: Cloudflare was named a Leader in 2022 GigaOm Radar Report for DDoS Protection

Cloudflare DDoS Protection: Cloudflare's DDoS protection services are designed to defend against and mitigate the impact of DDoS attacks, ensuring the availability and reliability of web applications.

Cloudflare SSL: Cloudflare offers SSL encryption to secure data transmission between clients and servers, protecting sensitive information and complying with security best practices.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution fully adheres to the requirement of being scalable to meet the needs of Florida's multi-tenant enterprise. We

designed our CDN solution to provide the flexibility and agility required to adapt to varying resource demands.

Cloudflare Network: Cloudflare operates a highly scalable global network with numerous data centers strategically distributed worldwide. This expansive infrastructure enables us to efficiently scale resources and handle increasing demands. Cloudflare's network being anycast by nature means that traffic is also sent to the closest Cloudflare point of presence (PoP) for inspection. If a PoP is down for maintenance, an ISP is down in path to Cloudflare, etc. Cloudflare will send incoming traffic to the closest available facility. This ensures we are always online and always able to deliver traffic to your organization.

Multi-Tenancy: Cloudflare provides flexibility in how organizations can adopt a true multi-tenancy model. Each unique agency is able to have a completely separate account with completely separate configurations. The users within that account would not have access to other accounts unless that is desired by the State of Florida. A common approach we see states adopt is one in which a small group of "Super admins" have access to all tenants within Cloudflare while tenant specific users are only able to access their own configurations, analytics, etc. Layer role-based access controls on top of this, and you are able to fully restrict the scope of what an administrative user has access to, where configuration changes will apply, and what configuration changes a user could potentially have access to make.

Cloudflare Load Balancing: Cloudflare offers Load Balancing services that allow enterprises to distribute traffic across multiple resources, ensuring scalability and high availability. This capability enables quick addition or removal of resources based on demand. By leveraging our global network and load balancing services, Cloudflare enables enterprises to scale their resources efficiently, add or remove resources quickly based on demand, and deliver content reliably to end-users.

We understand the importance of scalability for multi-tenant enterprises, and our CDN solution is specifically designed to meet their evolving needs while ensuring optimal performance and reliability.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of delivering content quickly and efficiently to end-users. Our CDN

solution is designed to optimize content delivery by leveraging multiple points of presence (PoPs) strategically located around the world, including the United States of America. This ensures that content is delivered from the closest server to the end-user, minimizing latency and enhancing performance. Here are the relevant links supporting this statement:

Cloudflare CDN: Cloudflare operates a global network of data centers across various locations, known as points of presence (PoPs). This extensive network infrastructure allows us to deliver content quickly and efficiently to end-users worldwide.

Cloudflare Network: Cloudflare's network spans across over 485 data centers strategically distributed worldwide, of which 90+ Data Centers reside in the U.S. These points of presence (PoPs) are designed to ensure that content is delivered from the closest server to the end-user, reducing latency and optimizing performance.

Cloudflare Anycast: Cloudflare utilizes Anycast routing technology, which directs user requests to the nearest Cloudflare POP. This routing method enables efficient content delivery by minimizing the distance between end-users and the content they are accessing.

By leveraging our global network of PoPs and Anycast routing technology, Cloudflare's CDN solution enables quick and efficient content delivery to end-users. Our infrastructure is designed to minimize latency, optimize performance, and ensure a seamless user experience.

Cloudflare's CDN solution has the capability to deliver content quickly and efficiently from the closest server to end-users.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement by allowing customization of caching rules, SSL certificates, and other settings to meet the specific needs of Florida. Our CDN solution provides extensive customization options, empowering enterprises to tailor the CDN configuration according to their unique requirements.

Cloudflare CDN: Cloudflare's CDN solution offers comprehensive customization capabilities, allowing government and educational enterprises to define caching rules - such as how long to cache, what content to cache, when to purge cache, etc.... This flexibility ensures that the CDN is configured to meet the specific needs of each enterprise.

Cloudflare Transform Rules: Allow for requests to be modified "mid-flight" through Cloudflare. Configurations for things like redirects, server-side rewrites, and appending / removing headers can all be managed via the UI or the API.

Cloudflare SSL: Cloudflare offers customizable SSL certificate options, including the ability to upload custom certificates, have Cloudflare issue certificates, modify SSL parameters like cipher suites & minimum TLS standards, and even force all traffic to use HTTP(s) that arrives at Cloudflare's edge.

Cloudflare understands that every enterprise has unique requirements, and our CDN solution provides the necessary flexibility for customization. With features such as Page Rules and customizable SSL certificates, enterprises can define caching behaviors, tailor security settings, and modify other configurations to align with their specific needs.

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.

Response: Cloudflare's solution adheres to the requirement to allow administrators the control of access to the solution, the ability to set permissions, and manage user accounts. Cloudflare supports granular role based access controls to ensure administrators are only admitted access to the controls relevant to their function. This same principle can also be extended to API tokens and scoping permissions to only the functions an admin needs. Cloudflare also supports SSO integration to any identity provider to allow organizations to leverage their existing identity accounts / any MFA mechanisms they would like.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution fully adheres to the requirement of delivering a wide range of content types. Our CDN solution is designed to handle various content types, including static content, dynamic content, and streaming media.

Cloudflare CDN: Cloudflare's CDN solution is able to maximize performance by delivering static content such as images, CSS files, and JavaScript files to client's from the closest Cloudflare point of presence. These files are cached and distributed across the global network, ensuring quick and reliable content delivery. Cloudflare deems some content as dynamic (ex. HTML) and would not by default cache the asset;

however, organizations have full flexibility and control to instruct Cloudflare to proceed with caching dynamic assets.

Cloudflare Stream: Cloudflare Stream is a video streaming platform that enables seamless delivery of streaming media content. It provides adaptive bitrate streaming, secure video playback, and customizable video player options.

Cloudflare's CDN solution handles a diverse range of content types, catering to the needs of enterprises with static content, dynamic content, and streaming media. Whether it's serving static assets efficiently, processing dynamic content at the edge, or delivering streaming media reliably, Cloudflare provides the necessary capabilities to ensure an optimal content delivery experience.

6.1.7. Caching

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

Response: Cloudflare's Content Delivery Network (CDN) solution fully adheres to the requirement of caching content at the edge to reduce origin server load and improve performance. Our CDN solution is specifically designed to leverage edge caching, providing benefits such as reduced latency and enhanced content delivery.

Cloudflare CDN: Cloudflare's CDN solution employs robust edge caching mechanisms. By caching content at the edge locations of our global network, we significantly reduce the load on the origin server, resulting in improved performance and faster content delivery.

Cloudflare Caching: Cloudflare offers various caching features, including static content caching, dynamic content caching, and content expiration controls. These caching capabilities optimize content delivery, reduce the need for frequent origin server requests, and enhance overall performance.

Cloudflare's CDN solution excels at caching content at the edge, alleviating the load on origin servers and significantly improving performance. By leveraging our global network of edge locations, we ensure that content is delivered swiftly to end-users while minimizing the need for repeated requests to the origin server.

Cloudflare's edge caching capabilities bring the benefit of reducing origin server load and enhancing 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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of protecting against Distributed Denial-of-Service (DDoS) attacks by filtering out malicious traffic and redirecting legitimate traffic to the origin server. Our CDN solution includes robust DDoS protection measures to ensure the availability and integrity of services. We see a multitude of different DDoS attacks and are able to help protect customers from L3, L4, & L7 DDoS attacks with our platform.

Cloudflare DDoS Protection: Cloudflare provides advanced DDoS protection capabilities that mitigate and filter out malicious traffic, ensuring uninterrupted access to web applications and resources. By leveraging a combination of network-level and application-level protections, Cloudflare safeguards against various types of DDoS attacks.

Cloudflare's DDoS protections leverage both real-time signatures indicative of DDoS traffic, and the ability to do an adaptive analysis of the unique traffic to a customer's account to better both identify and mitigate the threat.

Cloudflare DDoS: :Cloudflare was named a Leader in 2022 GigaOm Radar Report for DDoS Protection

Optional addition - Cloudflare Magic Transit: Cloudflare's Magic Transit is designed to protect entire networks from DDoS attacks. By routing traffic through Cloudflare's global network, it enables the filtering and mitigation of DDoS attacks closer to the source, preventing them from reaching 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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of balancing traffic across multiple origin servers to prevent server overload. Our CDN solution offers robust traffic balancing capabilities, ensuring optimal distribution of traffic and maintaining the availability and performance of services.

Cloudflare Load Balancing: Cloudflare's Load Balancing feature enables the distribution of incoming traffic across multiple origin servers, ensuring efficient resource utilization and preventing any single server from being overloaded. Load Balancing can be configured with various algorithms and health checks to optimize traffic distribution.

Cloudflare Traffic Manager: Cloudflare Traffic Manager provides intelligent routing capabilities, allowing administrators to direct traffic to the most suitable origin server based on various criteria such as location, capacity, and performance. This dynamic traffic routing ensures load balancing and optimal utilization of resources.

Cloudflare's load balancer supports steering policies for Active/Passive and Active/Active setups, as well as the ability to route a request to an origin via the most performant route / the most geographically close origin.

With Cloudflare, the State of Florida can customize traffic handling logic at the edge. This flexibility allows for advanced traffic routing and load balancing strategies tailored to specific needs, providing fine-grained control over traffic distribution.

6.1.10. Real-time Monitoring

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

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of providing real-time monitoring of traffic, usage, and security incidents. Our CDN solution incorporates comprehensive monitoring capabilities to ensure visibility into network activity, usage patterns, and security events in real-time.

Cloudflare Analytics: Cloudflare Analytics provides real-time visibility into website traffic, including data on visitors, bandwidth usage, request rates, and more. This monitoring capability allows enterprises to gain insights into their traffic patterns and make informed decisions.

Cloudflare Firewall Events: Cloudflare Firewall Events provides real-time monitoring and logging of security incidents, including detailed information about potential threats, attacks, and rule matches. This enables enterprises to identify and respond to security incidents promptly.

Cloudflare Radar: Cloudflare Radar offers insights into various security events and trends observed across the Cloudflare network. It provides real-time intelligence on threats, attacks, and vulnerabilities, allowing enterprises to stay informed and proactively respond to emerging security risks.

Cloudflare's CDN solution includes robust monitoring capabilities through tools like Analytics, Firewall Events, and Radar. These features enable enterprises to monitor traffic, usage, and security incidents in real-time, empowering them to identify and address any anomalies, optimize performance, and respond promptly to security threats.

The information above highlight's Cloudflare's real-time monitoring capabilities and how they contribute to tracking traffic, usage, and security incidents within our CDN solution.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of providing tools to optimize content delivery, including image compression and minification of HTML, CSS, and JavaScript. Our CDN solution includes a suite of performance optimization features that improve content delivery efficiency.

Cloudflare Image Optimization: Cloudflare's Image Optimization automatically optimizes images by compressing them without sacrificing quality. This feature reduces image file sizes, resulting in faster load times and improved content delivery.

Cloudflare AutoMinify: Cloudflare's AutoMinify feature automatically minifies HTML, CSS, and JavaScript resources. Minification removes unnecessary characters and spaces from these files, reducing their file sizes and improving page load times.

Cloudflare Rocket Loader: Cloudflare's Rocket Loader optimizes the delivery of JavaScript files by asynchronously loading and prioritizing them. This feature improves page rendering times and overall content delivery performance.

Cloudflare's CDN solution provides powerful tools for optimizing content delivery. With features such as Image Optimization, AutoMinify, and Rocket Loader, we enable businesses to reduce file sizes, improve load times, and enhance the overall performance of their web content.

The information above highlights Cloudflare's content optimization capabilities and how they contribute to improving content delivery efficiency, including image compression and minification of HTML, CSS, and JavaScript resources.

6.1.12. Onboarding

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

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of including a staging environment for onboarding and changes. Our CDN solution offers a staging environment that enables businesses to safely test and validate changes before deploying them to production.

By providing a staging environment, Cloudflare's CDN solution allows businesses to safely onboard new configurations, test changes, and validate their impact before deploying them to the live environment. This helps minimize risks and potential disruptions, ensuring a smooth transition and improved control over changes made to the CDN configuration.

6.1.13. Data Restricting

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

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of having the ability to contain/restrict data to the continental United States. Our CDN solution offers features and capabilities that allow businesses to implement data containment and restriction measures via geofencing. Cloudflare's solution will be FedRAMP moderate based on the entities needs, allowing traffic inspection within our FedRAMP Authorized Points of Presence. For those entities who choose to not be in Cloudflare's FedRAMP Authorized solution Cloudflare is including geo-fencing to customize the entities specific needs in our commercial cloud.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of supporting a multi-tenant, multi-organization architecture. Our CDN solution provides the necessary capabilities to enable each tenant to have its own instance while aggregating up to a single instance and view. Additionally, our solution includes dashboards that offer single-source visibility into threats, investigations, and trends for enterprise security operations. Whether the FLDS decides to consolidate into a single tenant, create tenancy hierarchy or divide tenants based on region or sector Cloudflare will accommodate the architecture.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of being provided as Software as a Service (SaaS) via cloud-hosted infrastructure. Our CDN solution is delivered through the cloud, ensuring that businesses have access to the latest releases of management server and endpoint agent software. Additionally, our solution enables capacity extensibility in the cloud with minimal impact on agent or management infrastructure.

Cloudflare CDN: Cloudflare's CDN solution is delivered as a cloud-based service, providing the benefits of SaaS. This approach ensures that businesses can easily access the latest releases of management server and endpoint agent software without the need for manual upgrades or maintenance.

Cloudflare Scalability: Cloudflare's infrastructure is designed to provide capacity extensibility in the cloud. As your needs grow, Cloudflare's scalable architecture allows for seamless scaling of resources, ensuring minimal impact on agent or management infrastructure.

Cloudflare's CDN solution, being offered as SaaS via cloud-hosted infrastructure, provides businesses with the advantages of automatic updates, continuous improvements, and the ability to leverage the latest software releases. Additionally, our scalable architecture ensures that businesses can easily extend capacity in the cloud without significant impact on the 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.

Response: Cloudflare does not provide an endpoint detection and response solution. Cloudflare's API first strategy provides a simple method for integrating with FLDS' vendor of choice.

6.1.17. Malware Prevention

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

Response: Cloudflare's WAF provides the ability to scan any content being uploaded to your applications via our reverse proxy. Content (ex. uploaded files) are scanned for malicious signatures like malware. The scan results along with the metadata are made available as fields in the WAF custom rules, which allows organizations to build fine-grained mitigation rules.

For more information regarding Cloudflare's WAF Uploaded content scanning.

This is not anti-malware at the endpoint, but anti-malware facilitated at Cloudflare's edge for any content uploaded to your applications.

6.1.18. Product Usability

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

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of providing easy-to-understand, friendly interfaces with intuitive designs to facilitate user engagement. Our CDN solution offers user interfaces that prioritize simplicity, usability, and intuitive design to enhance user engagement.

Cloudflare Dashboard: Cloudflare's user dashboard provides a user-friendly interface designed to make it easy for users to manage and configure their CDN settings. The dashboard offers a clean and intuitive design that facilitates user engagement and streamlines the management experience.

Cloudflare Apps: Cloudflare Apps is a marketplace of pre-built integrations and applications that can be easily added to the Cloudflare ecosystem. The Apps interface follows a user-friendly design, making it simple for users to explore and integrate additional functionality into their CDN solution.

Cloudflare Developer Documentation: Cloudflare's developer documentation provides clear and concise guides, tutorials, and examples to help users understand and utilize Cloudflare's CDN solution effectively. The documentation is designed to be user-friendly, aiding user engagement with the platform.

Cloudflare's CDN solution is built with a focus on user experience, offering easy-to-understand friendly interfaces with intuitive designs. Whether it's the user dashboard, the Apps marketplace, or the developer documentation, we strive to provide interfaces that are accessible, engaging, and facilitate seamless user interaction.

The information above highlights Cloudflare's user-friendly interfaces and intuitive designs, enabling user engagement and enhancing the overall user experience within our CDN solution.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of having an easy-to-use administration console and allowing straightforward ongoing management. Our CDN solution provides an intuitive administration console that simplifies the management and configuration process.

Cloudflare's CDN solution offers an easy-to-use administration console that simplifies ongoing management tasks. No agent is required for Cloudflare's solution.

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.

Response: This requirement does not apply to Cloudflare's CDN offered solution. Cloudflare's API first strategy provides a simple method for integrating with FL-DS's vendor of choice for this requirement.

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.

Response: Cloudflare is interoperable with all major modern Operating Systems and Browsers (including mobile devices). Cloudflare operates as a fully SaaS based platform. The "cloud, virtual, and container-based workloads" requirement does not apply to Cloudflare's CDN offered solution. Cloudflare's API first strategy provides a simple method for integrating with FL-DS's vendor of choice for this requirement.

6.1.22. Disaster Recovery and Backup

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

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement and is purpose built for enabling processes such as disaster recovery, rollbacks, and version control, so we can hold a 100% availability SLA. Our CDN solution provides features and capabilities that support these essential processes for content delivery.

Cloudflare is an anycast network with over 485+ points of presence around the world, 90 within the United States and has built in redundancy and the ability to scale the platform as needed due to our scale.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of providing required data storage capacity, file types, and locations, as well as processes such as disaster recovery, rollbacks, extraction, or eradication. Additionally, our CDN solution enables monitoring, reporting, and management of data sharing, along with encryption and security for data at rest and in motion.

Cloudflare Data Storage: Cloudflare's CDN solution provides ample data storage capacity to accommodate various file types and locations. With our global network of edge servers, content can be stored and delivered efficiently to end-users worldwide.

Cloudflare Workers KV: Cloudflare Workers KV allows businesses to store and retrieve data at the edge of the network, providing flexible storage options for different types of data. This feature supports processes like disaster recovery, rollbacks, and data extraction.

Cloudflare Logs and Analytics: Cloudflare's logs and analytics capabilities provide monitoring, reporting, and management functionalities for data sharing. Through detailed logs and analytics, businesses can gain insights into data usage, traffic patterns, and content delivery performance.

Cloudflare SSL/TLS Encryption: Cloudflare offers robust encryption and security measures for data at rest and in motion. Our SSL/TLS encryption ensures the confidentiality and integrity of data transmitted between end-users and origin servers.

Cloudflare's CDN solution provides the necessary data storage capacity, supports various file types and locations, and offers processes such as disaster recovery, rollbacks, extraction, and eradication. Additionally, our solution enables monitoring, reporting, and management of data sharing, while ensuring encryption and security for data at rest and in motion.

The information above highlights how Cloudflare's CDN solution addresses the requirements of data storage, disaster recovery, data management, encryption, and security within our content delivery infrastructure.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of providing capabilities such as user authentication, password policy management, two-factor authentication, single sign-on, and role-based access. Our CDN solution offers robust authentication and access control features to ensure secure and controlled access to content and resources.

Cloudflare Access Identity Providers: Cloudflare integrates with popular identity providers (IdPs) to enable seamless authentication and single sign-on experiences for users. This integration allows businesses to leverage existing identity management systems and enforce role-based access control.

Cloudflare's CDN solution provides a range of capabilities for user authentication, password policy management, two-factor authentication, single sign-on, and role-based access control.

The information above highlights how Cloudflare's CDN solution supports user authentication, password policy management, two-factor authentication, single sign-on, and role-based access control within our content delivery infrastructure.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of leveraging network technologies such as software-defined wide area networks (SD-WAN) and over-the-top (OTT) monitoring to ensure optimal performance. Our CDN solution harnesses advanced network technologies and monitoring capabilities to deliver exceptional performance.

Cloudflare Magic WAN securely connects your users, offices, data centers and hybrid cloud over the Cloudflare global network without relying on vendor-specific hardware or software.

Optional additions:

Cloudflare Magic Transit: Cloudflare Magic Transit combines DDoS protection, traffic acceleration, and advanced network monitoring to provide secure and reliable network

connectivity. It leverages SD-WAN principles to optimize performance and ensure the efficient routing of traffic.

Cloudflare Network Performance: Cloudflare's network is built on a global infrastructure that uses OTT monitoring to continuously measure performance and ensure optimal delivery of content. This includes monitoring latency, packet loss, and other key metrics to maintain high-quality network connectivity.

By leveraging SD-WAN technologies and employing OTT monitoring, Cloudflare's CDN solution optimizes performance and ensures efficient content delivery. With features like Cloudflare Magic Transit and our robust network infrastructure, we provide a reliable and high-performing solution.

The information above highlights how Cloudflare's CDN solution uses network technologies like SD-WAN and OTT monitoring to ensure the optimal performance of our content delivery infrastructure.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of complying with relevant standards such as the 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. Our CDN solution prioritizes data protection and privacy by complying with these standards and certifications.

Cloudflare Data Protection: Cloudflare is committed to data protection and privacy. We have implemented measures to comply with regulations such as GDPR, HIPAA, and CJIS, ensuring that customer data is handled with the highest level of security and privacy.

Cloudflare Compliance: Cloudflare has obtained various certifications, including SOC 2 Type II and ISO 27001, which validate our commitment to security, availability, and confidentiality of customer data. These certifications demonstrate our compliance with industry best practices and standards.

Cloudflare's CDN solution is designed with a strong focus on data protection and privacy compliance. By adhering to standards like GDPR, CJIS, HIPAA, and obtaining certifications such as SOC 2 and ISO 27001, we ensure that customer data is handled securely and in accordance with industry best practices.

Cloudflare's solution is FedRAMP moderate, allowing traffic inspection within our FedRAMP Authorized Points of Presence. In the case of an entity choosing to not be in our FedRAMP Authorized option these certifications still apply; GDPR, CJIS, HIPAA, and obtaining certifications such as SOC 2 and ISO 27001.

The information above highlights how Cloudflare's CDN solution complies with relevant data protection standards and certifications, safeguarding customer data and ensuring regulatory 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.

Response: Cloudflare meets this requirement. Cloudflare provides granular tools to scope any level of resource deployment across our platform. We have third party integrations with Terraform as well as API endpoints, which can be used to extract and maintain configurations completely through a modern DevOps model.

Cloudflare has a custom built-in analytics platform which allows users to configure data, telemetry, security events, and notifications to a desired specification. All changes in the system are actively tracked, with the ability to export audit logs as needed. Controls and boundaries can be set by service, further supporting a “least privileged access” security framework for business needs.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of integrating with the Department's existing security tools such as firewalls, antivirus software, endpoint management solutions, and security information and event management (SIEM) systems. Our CDN solution is designed to seamlessly integrate with a wide range of security tools and systems to enhance the overall security posture.

Cloudflare Partnerships: Cloudflare collaborates with various technology partners, including leading security vendors, to ensure compatibility and integration with their solutions. This allows for a comprehensive security ecosystem that works together seamlessly.

Cloudflare Logpush: Cloudflare Logpush enables customers to export their CDN logs to SIEM systems or log analysis tools of their choice. This integration facilitates centralized monitoring and analysis of security events alongside other system logs.

Cloudflare API: Cloudflare provides a robust API that allows for seamless integration with existing security tools and systems. The API offers a wide range of functionalities, including managing firewall rules, configuring DNS settings, and controlling various aspects of the CDN solution.

Cloudflare WAF & API Protection: Cloudflare's WAF was named a leader in Gartner's 2022 Magic Quadrant for Web Application & API Protection.

Cloudflare's CDN solution is designed to be flexible and adaptable, allowing for integration with the Department's existing security tools. Whether it is integrating with firewalls, antivirus software, endpoint management solutions, or SIEM systems, Cloudflare works closely with customers to support their specific integration requirements.

The information above highlights how Cloudflare's CDN solution integrates with existing security tools and systems, enabling a unified and cohesive security infrastructure.

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).

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of being capable of data integration through common exchange techniques and frameworks such as RESTful Application Programming Interfaces (APIs). Our

CDN solution provides robust APIs that enable seamless data integration and exchange with other systems and applications.

Cloudflare API Documentation: Cloudflare offers comprehensive API documentation that provides details on how to interact with the CDN solution using RESTful APIs. The API allows customers to programmatically manage and control various aspects of their CDN configuration and operations.

Cloudflare Data Streaming: Cloudflare's Data Streaming service allows customers to stream and collect logs in real-time, facilitating data integration with external systems for analysis and processing. The streaming capabilities provide a flexible and scalable solution for data exchange.

Cloudflare's CDN solution supports data integration through common exchange techniques and frameworks, including RESTful APIs. Our API documentation and data streaming service provide the necessary tools and capabilities for seamless data integration and exchange with other systems.

The information above highlights how Cloudflare's CDN solution facilitates data integration through RESTful APIs and other techniques, empowering customers to build powerful integrations and exchange data with ease.

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.

Response: Cloudflare will adhere to this requirement.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of initial integration, including connecting each customer to the state Cybersecurity Operations Center (CSOC) and validating with FLDS that all solution data is properly integrated, as requested by the customer. Our team will ensure that our CDN solution seamlessly integrates as well as collaborate with CSOC and FLDS to meet the specific integration requirements.

Cloudflare Enterprise: Cloudflare Enterprise provides dedicated support and tailored solutions for government customers. With our Enterprise offering, we work closely with customers to facilitate the integration process and will ensure the proper connection to CSOC and FLDS.

Cloudflare for Government: Cloudflare's solutions for government entities are designed to meet rigorous compliance and security requirements. Through our dedicated government offering, we have experience working with various agencies and departments to support their integration needs.

As part of our commitment to FLDS success, Cloudflare will collaborate closely with FLDS to establish the necessary connections between Cloudflare's CDN solution and the state Cybersecurity Operations Center. Cloudflare will ensure that all solution data is properly integrated and will validate the integration with FLDS to meet their requirements.

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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of initial integration, including connecting each customer to the state Cybersecurity Operations Center (CSOC) and validating with FLDS that all solution data is properly integrated, as requested by the customer.

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. 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.

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of performing in accordance with the approved Service Level Agreement (SLA) and being available 99.999% of the time per month. Our CDN solution is designed to deliver exceptional performance and availability, meeting the highest standards of reliability.

Cloudflare SLA: Cloudflare's 100% Uptime SLA outlines the commitments and guarantees for service availability and performance. We strive to maintain a high level of uptime, ensuring that our CDN solution is available to customers as agreed upon in the SLA.

Cloudflare Network Status: Cloudflare provides real-time status updates on the performance and availability of our network. By monitoring the network status page, customers can stay informed about any incidents or maintenance activities that might affect service availability.

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

Cloudflare's CDN solution is designed to provide high availability and performance, backed by our SLA commitments. With a robust infrastructure and a global network of data centers, we aim to deliver content efficiently and maintain exceptional uptime for our customers.

The information above highlights Cloudflare's SLA and network status, ensuring transparency and accountability in meeting service availability requirements.

Business Service Level Agreement ("SLA"). Cloudflare ("Company") commits to provide a level of service for Business Customers demonstrating:

100% Uptime. The Service will serve Customer Content 100% of the time without qualification.

Penalties. If the Service fails to meet the above service level, the Customer will receive a credit equal to the result of the Service Credit calculation in Section 10 of our SLA.

a) **DRAFT SLA**

RFQ Text:

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

Response: Cloudflare's Content Delivery Network (CDN) solution adheres to the requirement of performing in accordance with the approved Service Level Agreement (SLA) and being available 99.999% of the time per month. Our CDN solution is designed to deliver exceptional performance and availability, meeting the highest standards of reliability.

Cloudflare SLA: Cloudflare's SLA outlines the commitments and guarantees for service availability and performance. We strive to maintain a high level of uptime, ensuring that our CDN solution is available to customers as agreed upon in the SLA.

Cloudflare Network Status: Cloudflare provides real-time status updates on the performance and availability of our network. By monitoring the network status page, customers can stay informed about any incidents or maintenance activities that might affect service availability.

Cloudflare's CDN solution is designed to provide high availability and performance, backed by our SLA commitments. With a robust infrastructure and a global network of data centers, we aim to deliver content efficiently and maintain exceptional uptime for our customers.

b) **TRAINING & SUPPORT SLA**

RFQ Text:

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

Florida Digital Service
RFQ Title: Content Delivery Network (CDN) Solution
RFQ Number: DMS-22/23-156
Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

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).

Response: Cloudflare's Content Delivery Network (CDN) solution includes comprehensive technical support to assist with implementation, customization, and troubleshooting. We offer a range of support services to ensure a successful implementation of the solution and provide ongoing support to customers and FLDS.

Implementation is included in the cost of all Cloudflare services.

Cloudflare Support: Cloudflare provides dedicated technical support through various channels, including online resources, documentation, community forums, and direct contact with our support team. Our support services are designed to assist customers and FLDS with implementation, customization, and troubleshooting.

Cloudflare Implementation Services: Cloudflare offers implementation services, including consulting and training, to provide expert guidance and assistance during the implementation of the CDN solution. Our professional services team can work closely with customers and FLDS to ensure a smooth and successful implementation.

Cloudflare's CDN solution is backed by comprehensive technical support, including a dedicated support team, extensive documentation, and additional professional services if needed. We are committed to assisting customers and FLDS throughout the implementation process and providing ongoing support to ensure their success.

Cloudflare provides several resources to train users on its products and services. On top of those resources, the State will be provided a Client Success Manager and a Customer Success Engineer that will assist with live training during implementation and ongoing.

Cloudflare Learning Center: The Cloudflare Learning Center provides a wide range of articles, tutorials, and guides on various topics related to Cloudflare's products and services. It offers in-depth information to help users understand how to use and configure Cloudflare's solutions effectively.

Cloudflare Help Center: The Cloudflare Help Center offers comprehensive documentation and support articles that cover various aspects of Cloudflare's products and services. It provides step-by-step instructions, troubleshooting guides, and FAQs to assist users in understanding and resolving common issues.

Cloudflare Community Forum: The Cloudflare Community Forum is an online community where users can ask questions, share experiences, and learn from others using Cloudflare's products. It provides a platform for users to engage with each other and receive guidance from experienced community members.

c) IMPLEMENTATION PLAN

RFQ Text:

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

Response:

Cloudflare's proposal will include a range of support and resources to assist customers throughout the implementation process.

Dedicated Support Team: Cloudflare provides a dedicated support team that is available to assist customers with any questions, issues, or technical challenges during the implementation and initial integration phase. Our support team is knowledgeable and experienced in working with customers to ensure a smooth and successful deployment of the CDN solution.

Technical Documentation and Guides: Cloudflare offers comprehensive technical documentation, guides, and step-by-step instructions that provide detailed information on how to implement and integrate the CDN solution. These resources serve as valuable references for customers and provide guidance on best practices.

Implementation Services: Cloudflare's Implementation Services team offers additional support for customers who require expert guidance or hands-on assistance with the implementation and initial integration. This service can include consulting, customized training, and dedicated support to ensure a successful deployment.

Cloudflare Community Forum: The Cloudflare Community Forum is an online platform where customers can engage with fellow users, share experiences, and seek guidance. It is a valuable resource for customers to connect with the larger Cloudflare community and receive advice and support during the implementation process.

Cloudflare's support resources and services are designed to provide the State with the necessary assistance and guidance to ensure a successful implementation and initial integration of our CDN solution. Whether the State needs direct support from our dedicated team, access to technical documentation, engagement with the community, or the expertise of our Professional Services team, Cloudflare is committed to providing comprehensive support throughout the entire process.

This implementation plan will be further tailored through Scoping Sessions with FL[DS] Team.

Implementation Plan, Introduction and Cloudflare Mission

This document defines a migration proposal by the Cloudflare Migration Services team for FL[DS].

Cloudflare's migration mission is to provide an efficient way to transition to Cloudflare's platform and implement a plan for our customers to take full advantage of Cloudflare services for their environment. Cloudflare has taken deliberate measures to provide a robust toolset that improves usability; the design of the user interface and support infrastructure was created to facilitate this goal. This improves customer satisfaction due to the low maintenance and reliance on any third-party services.

This document is to serve as a guide to the migration process and includes details around project scope, timelines, responsibilities and expectations.

Florida Digital Service
RFQ Title: Content Delivery Network (CDN) Solution
RFQ Number: DMS-22/23-156
Date Due: May 23, 2023, 5:00 PM EST

All Cloudflare technology and software is proprietary. We do not require any hardware to be deployed.

Cloudflare’s Support Services

As part of Cloudflare’s Premium Success, customers receive a dedicated Customer Success Manager (CSM), a dedicated Customer Solutions Engineer (CSE), dedicated Account Executive, and 24/7 Emergency Phone Support. We are committed to providing ongoing training and guidance of the Cloudflare environment. This core team will provide regular business reviews and assure your success.

Broad Timeline

Contract Service Date - June 30, 2023

Kick-off meeting - TBD

Onboarding, Testing, and Migration - TBD, 1 - 3 months

Final Cut-Over - TBD

Within Scope

- Any action or activity that is implemented within the Cloudflare platform
- Process development that directly impacts Cloudflare’s products
- API calls that directly impact Cloudflare’s products
- IP management that is interfaced through Cloudflare’s platform
- The purchase and management of SSL certificates as it applies to Cloudflare’s SSL policies

Not Within Scope

- The development of any code outside of Cloudflare’s platform
- The development of processes that do not directly interface with Cloudflare’s products
- The final DNS configuration from an outside provider
- Advice or guidelines not related to Cloudflare’s core expertise

Project Approach



Florida Digital Service
RFQ Title: Content Delivery Network (CDN) Solution
RFQ Number: DMS-22/23-156
Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

Scoping & Training: The scoping phase lays out the groundwork for later phases of the project by establishing the objectives of the project, the scope, the staffing and provides education for the key members of the project team. During this phase, each business unit will help identify critical requirements and prioritize them for a successful implementation. A key output of this phase is a detailed migration plan or statement of work to act on.

Configuration: In the configuration phase, a migration plan has been developed and configuration settings may be adjusted to meet the requirements laid out in the prior phase. During configuration, Cloudflare and Business Process Owners will collaborate and review current settings together. Configuration may include setting up an endpoint, developing best practices, reviewing process improvements and reducing waste. A key output for this phase is a fully-reviewed configuration and identified roles and permissions.

Deployment: In the deployment phase, DNS records are added to the Cloudflare platform, roles and permissions have been entered. Settings identified in the Configuration phase can now be implemented into Cloudflare. TLS certificates can be issued during this phase and Worker development (if applicable) can be drafted. A key output for this phase is a fully configured Cloudflare organization. Security rules can be implemented at the end of this phase.

Staging: In the staging phase, DNS records, TLS certificates and applications are staged for testing. Customer business process owners (BPOs) can now begin a full validation and testing of accurate configurations within Cloudflare. Tuning sessions can be done during this phase.

Confirmation: In the Confirmation stage, all tests have been completed, and there is a high confidence that traffic being proxied through Cloudflare will be transited as expected. DNS records can now be updated to proxy traffic.

Continuous Improvement: In the Continuous Improvement phase, monitoring of traffic is critical. Any abnormal behavior or security risks will be reviewed and optimized on an ongoing basis. Full training sessions will be completed to assure all stakeholders understand how Cloudflare is operated.

Project Team

It is our experience that when Cloudflare and the Customer share responsibility for implementation, the project is successful. This SOW is created with the assumption of joint staffing and ownership of the implementation project.

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

Role	Responsibilities
Cloudflare Resources	
Customer Success Manager (CSM)	Cloudflare will provide a CSM to the implementation. The CSM will provide a leadership role on the project team to serve as the escalation point for the Customer and project team. Responsible for managing Cloudflare resources and adherence to project plan as well as any risk and implementation issues that may need to be addressed
Solution Engineer (SE)	Cloudflare will provide an SE to the implementation. Primary technical resource responsible for deployment, troubleshooting or any other guidance around edge architecture. Cloudflare may assign more than one SE depending on workload.
Account Executive (AE)	Cloudflare will provide an Account Executive to assist with ongoing strategy as it relates to your environment including: new product adoption, trial and POC requests, and commercial questions.
Customer Support	<p>Cloudflare offers a 24/7 follow-the-sun model support team. They are the primary contact in the event of urgent issues.</p> <p>How to contact:</p> <p>Create a support ticket and get a hold of Support Engineers by emailing entsupport@cloudflare.com</p> <p>Call Cloudflare Emergency NOC line for critical issues or attacks: +1 (650) 353-5922</p>
FL[DS] Resources	

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST



<p>TBD</p>	<p>Ideally 1 - 2 representatives - Cloudflare. Responsible for identifying technical and process requirements for their respective business units. Owners will be able to facilitate and approve of processes and ensure success of the overall project.</p> <p>Tasks include: Decision making for configurations as related to the unit, define processes, perform user testing</p>
------------	--

Task & Training Breakdown

The first part of our collaboration will focus on broad training for all relevant business process owners at FL[DS] on the general Cloudflare functions (Accounts, DNS, Security, WAF, LB). Following this, the migration will focus on the critical endpoints and the multi cloud deployment model. We will document the requirements and the agreed upon configurations for the priority use case roll out. Afterwards, a templated process will be shared with and applied to any remaining use cases.

Phase 1: Training

Training will be in the form of a virtual training session, training collateral, conference calls and/or recorded webinars.

Deliver to all:

- Account Overview
- Enterprise Support Services
- Role-based Access
- General Dashboard navigation
- Core Features
 - DNS
 - SSL
 - Security (WAF) settings
 - DDoS

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST



- Bots
- Load Balancing
- Rate Limiting
- Analytics

Phase 2: Standard Activities

SERVICE	DESCRIPTION	Owner	Completion Notes	Target Date
Configuration				
Data Export	Export DNS files into BIND compatible format for upload Export iRule (LB) config for review with Cloudflare team			
Proxy Configuration Review	Review current configurations and identify and prioritize specific line items			
Review Role-based Access Controls	Identify who should have access to which endpoints and read/write permissions			
Training				
Product Refresher	DNS / SSL / Load Balancing	Cloudflare	Notes: <i>Technical training and</i>	

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST



			<i>walkthrough Cloudflare dashboard for configuration and deployment scenarios with consideration focused on FL[DS] use cases.</i>	
Product Refresher	Security Features	Cloudflare	<p>WAF:</p> <p>OWASP Ruleset</p> <p>Managed Rules (managed by CF Engineering team)</p> <p>Firewall rules: Custom built firewall rules unique to your environment</p> <p>Bots: Build security posture towards un-verified automated traffic</p>	
Testing				
Endpoint Creation	Create Domains on Cloudflare			
Add TXT/CNAME Records	Verify domain ownership for Cloudflare and SSL Certificates			
Security Configurations	Whitelist Cloudflare IP space at origin infrastructure ingress point (firewalls / load balancers)		These can be staged with the support of the Cloudflare team.	

	<p>Identify baseline security configurations for WAF and Rate Limiting capabilities.</p> <p>Develop any needed automation for future deployments or DevOPS needs</p>			
Performance Configurations	<p>Take Proxied configuration settings and define:</p> <ul style="list-style-type: none"> - Default policies - Cache purge capabilities - Load Balancers - Cache-Tag usage and deployment - Geo-Specific Cache Controls to meet International regulations - API integration - SIEM integration 		<p>These can be staged with the support of the Cloudflare team.</p>	
Staging				
Functional Testing	<p>Complete application tests and adjust configurations as</p>			

	necessary. Assure that DNS request headers and responses are adequate			
Verify SSL	Verify edge and origin certificates are up to date.			
Security Review	Perform review and assessment of any security policies (including DDoS)			
Confirmation				
Update DNS	Switch DNS to begin proxying traffic <i>Either make Cloudflare authoritative DNS or Point an application's DNS via CNAME to Cloudflare</i>			
Continuous Improvement				
Terraform Compatibility	Assess compatibility with Terraform for potential future infrastructure update			
Monitoring and tuning	Monitor traffic and tune as necessary Consult and review CDN/cache settings for			

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST



	all domains (page specific TTL, host header override, etc)			
Monitoring & uptime	Cloudflare will indicate 100% uptime for the customer each month unless the customer identifies an incident (verified by Cloudflare) that caused downtime to their sites.			
Security Tuning	If Security is in a "simulate" mode, monitor triggers and turn on full blocking mechanisms			

Sample Task Driven Deployment Workflows

DNS

Task	Activity	Cloudflare Recommended Action	Notes
Onboarding (discussion)	Full Setup vs CNAME	<ul style="list-style-type: none"> Discuss the difference between Full Setup and CNAME Discuss the process to convert from CNAME to Full in the future 	<ul style="list-style-type: none"> For more information on setting up a CNAME partial setup, see here For more information on converting a CNAME setup to a full setup, see here
Onboarding (Core)	Full setup	<ul style="list-style-type: none"> Import BIND file Check records for completeness Start with records set to DNS only (to avoid downtime due to missing edge certificate) HOLD: Only during go-live Change nameservers 	<ul style="list-style-type: none"> For AWS/Route 53: <ul style="list-style-type: none"> use cli-53 (3rd party, make customer aware, no liability) to export zone files. Replace

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST

		<ul style="list-style-type: none"> Check nameservers change propagation 	<p>AWS-proprietary ALIAS records (CNAME)</p> <ul style="list-style-type: none"> Skip record scan, especially when migrating from another Cloudflare account (edge IPs imported otherwise) You can pause Cloudflare to temporarily switch all DNS records to DNS only
	CNAME setup	<ul style="list-style-type: none"> Add TXT activation record at the authoritative DNS provider Wait for activation Only add DNS records for hostnames that should be proxied (avoid confusion). If converting from a Full setup, remove records that will no longer work (TXT, MX, etc.) <p>HOLD: Only during go-live</p> <ul style="list-style-type: none"> Point from authoritative to Cloudflare via CNAME record 	<ul style="list-style-type: none"> Common gotchas: <ul style="list-style-type: none"> typing record instead of copy/pasting, resulting in typos or look-alike characters Many DNS providers implicitly append domain names. Most record types (TXT, MX, etc.) are not available here, as we cannot respond to queries when not authoritative (no CNAME delegation)
Onboarding (“optional”)	CNAME Flattening	<ul style="list-style-type: none"> Advise/overview of feature 	
	DNSSEC	<ul style="list-style-type: none"> Advise/overview of feature 	

CDN

Task	Activity	Cloudflare Recommended Action	Notes
------	----------	-------------------------------	-------

Review CDN documentation and default caching behavior	Caching by file extensions	<ul style="list-style-type: none"> Review origin + server configurations 	
	Cache-Control header and how Cloudflare respects the origin's caching header settings	<ul style="list-style-type: none"> Review origin + server configurations 	
	Page Rules in relationship with Caching options, TTLs, Edge vs Origin vs Browser caching terminology	<ul style="list-style-type: none"> Review current cache/hit ratio and decide what else can be cached from origin + server configurations 	
	Explain cache response headers: HIT, MISS, DYNAMIC, etc.	<ul style="list-style-type: none"> Review origin + server configurations based on these added headers 	
	Example of a Cache Everything Page Rule	<ul style="list-style-type: none"> Determine if any dynamic content should be cached by Cloudflare and add appropriate cache everything page rule 	
	Purge Cache and its enterprise only options.	<ul style="list-style-type: none"> Review purging options. Make use of tags if feasible for ease of purging. Purge by prefix, or by URL preferably. Evaluate the consequences of "Purge Everything" in the sense of origin resources. 	

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST

WAF & DDoS Protection

Task	Activity	Cloudflare Recommended Action	Notes
Enable all WAF rulesets in logging mode	Enable Cloudflare Managed ruleset in "Log" mode	<ul style="list-style-type: none"> Deploy ruleset in "Log" mode for each zone 	
	Enable OWASP ruleset in "Log" mode	<ul style="list-style-type: none"> Deploy OWASP ruleset in "Log" mode 	
	(Optional) Deploy Cloudflare Leaked Credentials Check	<ul style="list-style-type: none"> Deploy Cloudflare Leaked Credentials Check in "Log" mode 	
Review whether WAF exceptions are needed	Add WAF exception for any traffic that should not be evaluated by the WAF	<ul style="list-style-type: none"> Deploy WAF exceptions 	
	Review different options for bypassing the WAF	<ul style="list-style-type: none"> For a specific subset of traffic bypass a single rule, multiple rules, or an entire ruleset 	
Review Security Events	Review all security events	<ul style="list-style-type: none"> Make any adjustments to security settings based on any potential false negatives or false positives 	

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

DDoS Mitigation	Review default DDoS mitigation behavior	<ul style="list-style-type: none"> Review whether any overrides are needed within the DDoS managed rulesets 	
-----------------	---	--	--

Bots

Task	Activity	Cloudflare Recommended Action	Notes
Review Cloudflare Bot Scoring Model	Review Bots Analytics	<ul style="list-style-type: none"> Analyze existing traffic in Bot Analytics view 	
	How is automated traffic currently impacting your site(s)	<ul style="list-style-type: none"> Review all traffic scored <30 to see definitive automated traffic 	
Simulate Bot Mitigations	Built custom rule leveraging bot score to target automated traffic	<ul style="list-style-type: none"> Create custom rule with an action to log to start simulating what traffic Cloudflare would potentially action 	
		<ul style="list-style-type: none"> Identify any false positives using Firewall Analytics. Create exceptions 	
Stop Bad Automated Traffic	Enable Bot Mitigation	<ul style="list-style-type: none"> Modify existing Bot custom rule(s) to leverage the Managed Challenge action 	

Load Balancing

Task	Activity	Cloudflare Recommended Action	Notes
F5 / AVI EPS Migration	Review existing configurations in F5 & AVI EPS and where relevant migrate over	<ul style="list-style-type: none"> Export relevant configurations in existing LB solutions. iRules, Health Checks, etc... 	These configurations can be parsed and either manually added to Cloudflare or programmatically via our API

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

	configs		
Create Load Balancer	Configure Origin Pools / Origin nodes	<ul style="list-style-type: none"> Define server farms and traffic load between nodes 	
	Built Health Checks	<ul style="list-style-type: none"> Configure health checks to validate nodes are accessible 	Import health check logic from existing load balancing solutions
	Failover Logic	<ul style="list-style-type: none"> Decide between a standard failover, active: active, or performance / geo based failover model 	
	Custom Rules	<ul style="list-style-type: none"> If applicable - configure custom rules 	<p>Custom scenarios where traffic steering may differ</p> <p>Review existing iRules for potential import here</p>
Validate Health Checks	Ensure nodes are showing healthy before load balancing	<ul style="list-style-type: none"> Review Load Balancing analytics & origin pools 	
Go Live	Flow traffic through the Cloudflare Load Balancer	<ul style="list-style-type: none"> Mark Load Balancer as active in Cloudflare 	Load Balancers (when active) override DNS records

Detailed Timeline

TBD based on future discussions.

d) MDR SLA (OPTIONAL)

RFQ Text:

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

Response:

Florida Digital Service
RFQ Title: Content Delivery Network (CDN) Solution
RFQ Number: DMS-22/23-156
Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

e) FUTURE INTEGRATIONS SLA (OPTIONAL)

RFQ Text:

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

Response:

f) DISASTER RECOVERY PLAN

RFQ Text:

A draft disaster recovery plan per section 30.5.

Response: Cloudflare Disaster Recovery Overview:

Global Distributed Network Overview-

Cloudflare's edge network is designed to be resilient and fault tolerant. Our network of 250+ Points of Presence (PoPs) represent a true N+1 architecture where the failure of an individual PoP, or even several PoPs, will not compromise our fulfillment of services. Cloudflare employs Anycast routing to ensure web users are automatically routed to their nearest PoP and around any failures. The combination of this architecture and network produces a reliable, high-performance service. For up-to-date information related to the locations and status of the sites, please visit cloudflarestatus.com



Disaster Recovery

Florida Digital Service
RFQ Title: Content Delivery Network (CDN) Solution
RFQ Number: DMS-22/23-156
Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

With Cloudflare's resilient global network, the disaster recovery plan is focused on our Core Data Centers which are located in the West Coast of the United States and in the European Union. Core Data Centers house critical services including customer dashboard settings, product configurations, logs and analytics.

The geographically separate Core Data Centers allow Cloudflare Services to have continued operations during an adverse event. The Core Data Center located in the West Coast (US) is an active data center. In the event of a disaster that affects the active data center, Cloudflare will failover and continue operations from the EU data center.

Core Data Center Replications and Backups

Critical services are replicated between Cloudflare's Core Data Centers. During an adverse event, data can be sourced from any of the data center locations.

As an additional measure, databases are backed up daily and to an off-site location to ensure that Cloudflare has the ability to fully restore customer configurations if an adverse event impacted all of Cloudflare's Core Data Centers (US and EU).

Plan and Failover Tests

Cloudflare maintains a disaster recovery plan and performs testing and exercises at least annually to ensure recovery preparedness. The test stimulates a disaster and performs a cutover test by interrupting the replication between the two Core Data Centers and testing the ability to sufficiently restore the services in the EU. Test results are documented and reviewed by the Technical Teams for process improvements. Maintenance of our DR plan is examined by our external auditors.

The most recent DR exercise and tests were conducted 22 February - March 1, 2023. The Technical Teams were able to successfully failover critical services in the EU Core Data Center and then failback to the US Core Data Center. Established failover Recovery Point Objective (RPO) and Recovery Time Objective (RTO) were successfully met.

2) EXPERIENCE

RFQ Text:

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

Response: Below are two examples describing Cloudflare's experience of large scale customer deployments for similar solutions on a statewide basis or similar scale.

The State of Arizona deployed Cloudflare's Content Delivery Network, Web Application Firewall, DDoS Mitigation, Bot Management, and Rate Limiting.

State of Arizona outcomes

- Makes easily implemented, low-maintenance, and state-of-the-art Cloudflare layer-seven protection available to organizations with limited IT resources and funding
- Providing critical knowledge and tools empowering local agencies to implement and manage effective security infrastructures
- Secures websites and cloud-based agency applications across more than 80 domains against DDoS, JavaScript emulation, and other website vulnerabilities at the server level

The Department of Homeland Security / CISA has deployed Protected DNS, Registry and Authoritative DNS to the .gov TLD.

CISA's outcomes

- Unlike standard DNS resolvers, protective DNS resolvers check the hostname being resolved to determine if the destination is malicious. If that is the case, or even if the destination is just suspicious, the resolver can stop answering the DNS query and block the connection.
- As a team member on the CISA Task Order, Cloudflare will partner to help fortify federal government systems by blocking phishing and malware attacks before they happen and containing breaches that occur on devices, such as laptops and cell phones.
- Reducing the attack surface of .gov-related infrastructure and government organizations
- Automating sensitive portions of DNS security management, setting DNS records that make it hard to successfully impersonate the government in email by default, and offering new features
- Gaining visibility to better detect and prevent certain DNS ecosystem issues instead of reacting to them

3) IMPLEMENTATION

RFQ Text:

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

Response:

Below are two examples describing Cloudflare's experience of large-scale customer deployments for similar solutions on a statewide basis or similar scale. Cloudflare currently has over 4 million customers with over 179 TB of network capacity.

The State of Arizona deployed Cloudflare's Content Delivery Network, Web Application Firewall, DDoS Mitigation, Bot Management, and Rate Limiting.

State of Arizona outcomes

- Makes easily implemented, low-maintenance, and state-of-the-art Cloudflare layer-seven protection available to organizations with limited IT resources and funding
- Providing critical knowledge and tools empowering local agencies to implement and manage effective security infrastructures
- Secures websites and cloud-based agency applications across more than 80 domains against DDoS, JavaScript emulation, and other website vulnerabilities at the server level

The Department of Homeland Security / CISA has deployed Protected DNS, Registry and Authoritative DNS to the .gov TLD.

CISA's outcomes

- Unlike standard DNS resolvers, protective DNS resolvers check the hostname being resolved to determine if the destination is malicious. If that is the case, or even if the destination is just suspicious, the resolver can stop answering the DNS query and block the connection.
- As a team member on the CISA Task Order, Cloudflare will partner to help fortify federal government systems by blocking phishing and malware attacks before they happen and containing breaches that occur on devices, such as laptops and cell phones.
- Reducing the attack surface of .gov-related infrastructure and government organizations
- Automating sensitive portions of DNS security management, setting DNS records that make it hard to successfully impersonate the government in email by default, and offering new features
- Gaining visibility to better detect and prevent certain DNS ecosystem issues instead of reacting to them

4) VALUE-ADDED SERVICES

RFQ Text:

Detail regarding any value-added services.

Response:

Presidio is pleased to offer a free Cybersecurity Framework Workshop to FLDS and all participating Entities. This workshop can be branded as “FLDS powered by Presidio” or performed on an individual basis upon direction by FLDS.

We find that organizations need a comprehensive approach to cybersecurity, but it is challenging to know where to begin. With multiple, overlapping tools deployed in the enterprise, it can be difficult to see the whole picture. Cybersecurity talent and leadership are tough to recruit and retain. Frequent turnover has caused many gaps in enterprise strategies and solutions. Presidio’s workshop will help Entities understand how to leverage the tools they are receiving from the FLDS Local Grant Program, how they fit into their existing environment, and provide guidance on a broader Cybersecurity strategy and/or roadmap.

The Cybersecurity Framework Workshop (“CSF360”) is based on the NIST-CSF Framework and designed to help document and provide a consultative, flexible and comprehensive approach to security operations enterprise-wide.

Cybersecurity experts from Presidio lead a high-level discussion to identify risks and opportunities to improve an organization’s cybersecurity posture. We will lead a discussion and interview your team in a group setting. Our experts will help you find the gaps in your security technology solutions and business processes. We will document our findings in a live whiteboard session and provide our expert recommendations to improve security operations enterprise-wide.

The Presidio CSF360 Cybersecurity Workshop explores all areas of an organization’s cybersecurity situation. It forms the foundation of a deeper discussion of potential risk elements.

- Uses the industry standard NIST Framework methodology to help gauge organization’s cybersecurity maturity
- Brings together stakeholders from multiple IT disciplines to discuss key cybersecurity initiatives
- Helps the organization gain a 360-degree view of their cybersecurity posture in just a few short hours
- Provides a high-level deliverable upon Workshop completion with recommended actions

The Presidio CSF360 Cybersecurity Workshop is generally completed in 2-4 hours with the participation of key stakeholders in the organization.

KEY BENEFITS

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

Organizations who engage with Presidio's CSF360 Workshop have dramatically enhanced their cybersecurity posture.

- Organizations that may have a security project roadmap but no formal way of measuring progress
- Organizations that have done self-assessments but would like another pair of eyes to review their efforts
- Organizations that have policies but may not be following them as closely as they would like
- Organizations that have regulatory concerns

They have created consensus across their organization about the people, processes and tools required to protect their business.

- Security Leadership: CISO, CSO, CIO, CXO
- Security Team: Architecture, Engineering, Operations,
- SOC, Analyst
- Networking Team, Firewall Admins
- Data Center Team, Directory Server Admins, Email, Identity, Access
- Application Team, DevOps, SRE

With a short investment in time and exploring the current situation, organizations will benefit from having a common ground for cybersecurity risk management.

- A list of Cybersecurity activities that can be customized to meet the needs of any organization
- A complementary guideline for an organization's existing cybersecurity program and risk management strategy
- A risk-based approach to identifying cybersecurity vulnerabilities
- A systematic way to prioritize and communicate cost- effective improvement activities among stakeholders
- A frame of reference on how an organization views managing cybersecurity risk management

WHAT MAKES US DIFFERENT

Presidio is a trusted partner to our clients, securing their infrastructure, employees, clients, and assets from ever-growing cyber threats. Our clients trust Presidio:

- Highly Experienced team – Presidio's highly- credentialed cybersecurity consultants collectively have decades of combined practical experience spanning cyber security governance, architecture, and operations

Florida Digital Service
RFQ Title: Content Delivery Network (CDN) Solution
RFQ Number: DMS-22/23-156
Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

- Proven Cyber Leadership – Presidio has 15+ years of providing cybersecurity leadership and securing our nations’ most sensitive networks with specialization across many of the largest industry verticals
- Business Enablers – We understand cybersecurity should reduce risk to enable the success of your business, not serve as a roadblock to your success

WHY PRESIDIO

Presidio is a leading digital systems integrator, with deep experience in networking, cloud computing and broad hybrid infrastructures. Presidio recognizes that cybersecurity is foundational to the success of any business and has a highly specialized expert team at the ready. Our clients benefit from:

- Services methodology built on recognized industry standards including NIST, CIS, and ISO
- Compliance depth & breadth including PCI, HIPAA, NERC CIP, GDPR, CCPA, SOC 2, ISO 27001, DFARS 800-171, CMMC
- Multi-discipline experts provide for a broad view of client’s potential vulnerabilities
- Deep cybersecurity services bench and broad security services solutions provide domain expertise and consistent deliverables

Presidio Cybersecurity Practice covers a broad security services portfolio. Our highly skilled and tenured cybersecurity practitioners maintain leading industry certifications, provide thought leadership and practical industry experience. We have conducted thousands of engagements across all major industry segments. We look forward to the opportunity to serve Florida Digital Service.

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST



5) ATTACHMENT A – PRICE SHEET

RFQ Text:

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

Response:

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	<p>Initial Software Year</p> <p>One year of content delivery network software Solution as described in the RFQ per gigabyte (GB). To include:</p> <ul style="list-style-type: none"> • Implementation • initial training 	\$ <u>2.29</u>

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST



	<ul style="list-style-type: none"> • Initial Integration • integration maintenance • support services 	
2	<p>Subsequent Software Year</p> <p>One year of content delivery network software Solution as described in the RFQ per GB. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ <u>2.29</u>

Optional Renewal Term Pricing (Years 4-6)		
Item No.	Description	Rate Per GB
1	<p>Initial Software Year</p> <p>One year of content delivery network software Solution as described in the RFQ per GB. To include:</p> <ul style="list-style-type: none"> • Implementation • initial training • Initial Integration • integration maintenance • support services 	\$ <u>2.61</u>
2	<p>Subsequent Software Year</p> <p>One year of content delivery network software Solution as described in the RFQ per GB. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ <u>2.61</u>

IV. ACS Price Breakdown

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

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:

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
CF-CDN	Cloudflare Content Delivery Network		<i>Products enclosed here are included in the price per GB, Waterfall Pricing, Waterfall S-XL, & Enterprise Pricing Models</i>
CF-DDOS	Cloudflare Advanced DDoS Protection		
CF-WAF	Cloudflare Web Application Firewall		
CF-APP-SEC-ADV	Cloudflare Application Security Advanced		
CF-DNS	Cloudflare Managed DNS		
CF-ACM	Cloudflare Advanced Certificate Manager		
CF-BOTS	Cloudflare Bot Management		
CF-ALB	Cloudflare Load Balancer		
CF-PREM	Cloudflare Premium Success		
CF-GOV	Cloudflare Government Services (FedRAMP)		
Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
N/A	All Cloudflare SKUs include customer success implementation in this request.		

V. Waterfall Pricing (Optional)

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

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.

Section V. – Waterfall Pricing		
ACS SKU Number	ACS SKU Description	FLDS Price
CF-PERGB-BUNDLE1	Per GB 0-100,000 Bundle	\$2.29
CF-PERGB-BUNDLE2	Per GB 100,000-400,000 Bundle	\$2.05
CF-PERGB-BUNDLE3	Per GB 400,000-1,000,000 Bundle	\$1.72
Cloudflare Load Balancer	Per GB 1,000,000+ Bundle	\$1.43
* Based on verified CDN Bandwidth requirements. Tiers are retired based on aggregate consumption across all state entities.		
Section V. – Optional A la Carte Entity Bundle Pricing (S-XL Sizes)		
ACS SKU Number	ACS SKU Description	FLDS Price
CF-XL-BUNDLE	Cloudflare XL Bundle (Population 750K+)	\$286,072.00
CF-L-BUNDLE	Cloudflare L Bundle (Population 150K-750K)	\$114,555
CF-M-BUNDLE	Cloudflare M Bundle (Population 25k-150k)	\$57,338
CF-S-BUNDLE	Cloudflare S Bundle (Population 0-25K)	\$22,845
*If Sizing Unknown Pay for A la Carte Sizes and True Up After Year 1		

Bundles listed above are inclusive of the following services (listed in Section IV ACS Price Breakdown):

Cloudflare Content Delivery Network
Cloudflare Advanced DDoS Protection
Cloudflare Web Application Firewall
Cloudflare Application Security Advanced
Cloudflare Managed DNS
Cloudflare Advanced Certificate Manager
Cloudflare Bot Management
Cloudflare Load Balancer
Cloudflare Premium Success

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST



Cloudflare Government Services (FedRAMP)

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.

Section VI. – State of Florida Enterprise Pricing		
ACS SKU Number	ACS SKU Description	FLDS Price
CF-ENTAGR-YR1	Cloudflare Enterprise Agreement Year 1	\$6,006,752
CF-ENTAGR-YR2	Cloudflare Enterprise Agreement Year 2	\$6,006,752
CF-ENTAGR-YR3	Cloudflare Enterprise Agreement Year 3	\$6,006,752

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.

Presidio is offering a 2 – 4 hour Cybersecurity Workshop to each participating entity.

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.

Presidio Networked Solutions, LLC _____
 Vendor Name

Erik Hayko _____
 Signature

58-1667655 _____
 FEIN

Erik Hayko _____
 Signatory Printed Name

May 23, 2023 _____
 Date

Florida Digital Service
 RFQ Title: Content Delivery Network (CDN) Solution
 RFQ Number: DMS-22/23-156
 Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

6) ATTACHMENT B – CONTACT INFORMATION SHEET

RFQ Text:

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

Response:

ATTACHMENT B CONTACT INFORMATION SHEET

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:	Emily Phares	Emily Phares
Title:	Account Manager	Account Manager
Address (Line 1):	5337 Millenia Lakes Boulevard	5337 Millenia Lakes Boulevard
Address (Line 2):	Suite 300	Suite 300
City, State, Zip Code	Orlando, FL 32839	Orlando, FL 32839
Telephone (Office):	850-270-2988	850-270-2988
Telephone (Mobile):	850-524-3230	850-524-3230
Email:	ephares@presidio.com	ephares@presidio.com

Florida Digital Service
RFQ Title: Content Delivery Network (CDN) Solution
RFQ Number: DMS-22/23-156
Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

7) NON-DISCLOSURE AGREEMENT

RFQ Text:

Non-Disclosure Agreement executed by the vendor.

Response:

Presidio's signed NDA is included in the pages below.

Florida Digital Service
RFQ Title: Content Delivery Network (CDN) Solution
RFQ Number: DMS-22/23-156
Date Due: May 23, 2023, 5:00 PM EST

PRESIDIO®

ADDENDUM I

The following pages include Cloudflare information:

- Reference Architecture
- DDoS
- Web Application Firewall
- Bot Management
- Load Balancing
- Cloud Delivered Security
- Application Security Bundle
- Premium Success

Cloudflare CDN Reference Architecture



INDEX

Click to skip to each section

Overview	3
Traditional challenges deploying web applications	4-5
How a CDN tackles web application challenges	6
Introducing the Cloudflare CDN	7
Cloudflare CDN architecture and design	8-9
Argo Tiered Cache	9
Cloudflare Tiered Cache Topologies	10
Traffic flow: Argo Tiered Cache, Smart Tiered Cache Topology	11-12
Argo Smart Routing	12
Traffic Flow: Argo Tiered Cache, Smart Tiered Cache Topology	13-14
with Argo Smart Routing	
Summary	15

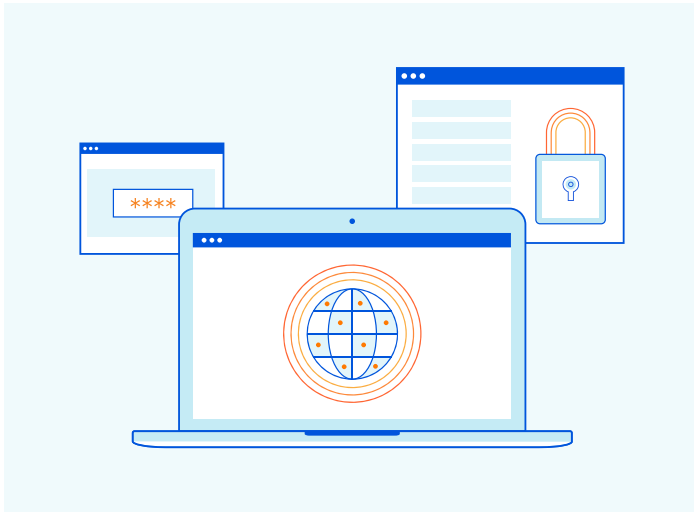
CLOUDFLARE CDN REFERENCE ARCHITECTURE

Overview

Every day, users of the Internet enjoy the benefits of performance and reliability provided by content delivery networks (CDNs). CDNs have become a must-have to combat latency and a requirement for any major company delivering content to users on the Internet. While providing performance and reliability for customers, CDNs also enable companies to further secure their applications and cut costs. This document discusses the traditional challenges customers face with web applications, how the Cloudflare CDN resolves these challenges, and CDN architecture and design.

CLOUDFLARE CDN REFERENCE ARCHITECTURE

Traditional challenges deploying web applications



Over the last several years, especially with the advent of the COVID-19 pandemic and the focus on remote work, there has been a significant growth in Internet traffic, further growing the need to efficiently manage network traffic, cut latency, and increase performance.

Companies running their applications in the cloud or on-premise are faced with the challenges of:

1. Implementing solutions to increase performance
2. As demand grows, scaling out their architecture to meet availability and redundancy concerns
3. Securing their environments and applications from growing Internet threats
4. Reining in growing costs related to doing all of the above

With companies serving customers across the globe, the above challenges require a significant undertaking. Traditionally, a website/application is deployed centrally and replicated to another region for availability, or the website/application is deployed across a handful of servers, sometimes across multiple data centers for resiliency.

The servers hosting the websites are called origin servers. When clients access a website, they make a request for resources from the server. Navigating to one website can generate hundreds of requests from the browser for HTML, CSS, images, videos, etc. With versions of HTTP prior to HTTP/2, each of these HTTP requests would also require a new TCP connection.

Enhancements in HTTP/2 allow for multiplexing multiple requests to the same server over a single TCP connection, thus saving server resources. However, compute and network resources are still consumed as servers respond to these requests. As more clients access the website, the following can result:

- The origin server starts to become overloaded with requests, impacting availability; companies start looking at scaling out to handle the additional load
- As each request has to make its way to the origin server, performance and user experience is impacted due to latency
- The latency for end users becomes proportional to the distance between the client and origin server, thus resulting in varying experiences based on client location
- As origin servers respond to the increasing requests, bandwidth, egress, and compute costs increase drastically
- Even as customers scale out to handle the increased demand in traffic, they are left exposed to both infrastructure-level and application-level distributed denial-of-service (DDoS) attacks

CLOUDFLARE CDN REFERENCE ARCHITECTURE

Traditional challenges deploying web applications (continued)

In Figure 1 below, there is no CDN present and there is an origin server sitting in the US. As clients access the website, the first step is DNS resolution, typically done by the user's ISP. The next step is the HTTP request sent directly to the origin server. The user experience will vary depending on their location. For example, you can see the latency is much lower for users in the US, where the origin server is located. For users outside the US, the latency increases, thus resulting in a higher round-trip time (RTT).

As more clients make requests to the origin server, the load on the network and server increases, resulting in higher latency and higher costs for resource and bandwidth use.

From a security perspective, the origin server is also vulnerable to DDoS attacks at both the infrastructure and application layer. A DDoS attack could be initiated from a botnet sending millions of requests to the origin server, consuming resources and preventing it from serving legitimate clients.

Further, in terms of resiliency, if the origin server temporarily goes offline, all content is inaccessible to users.

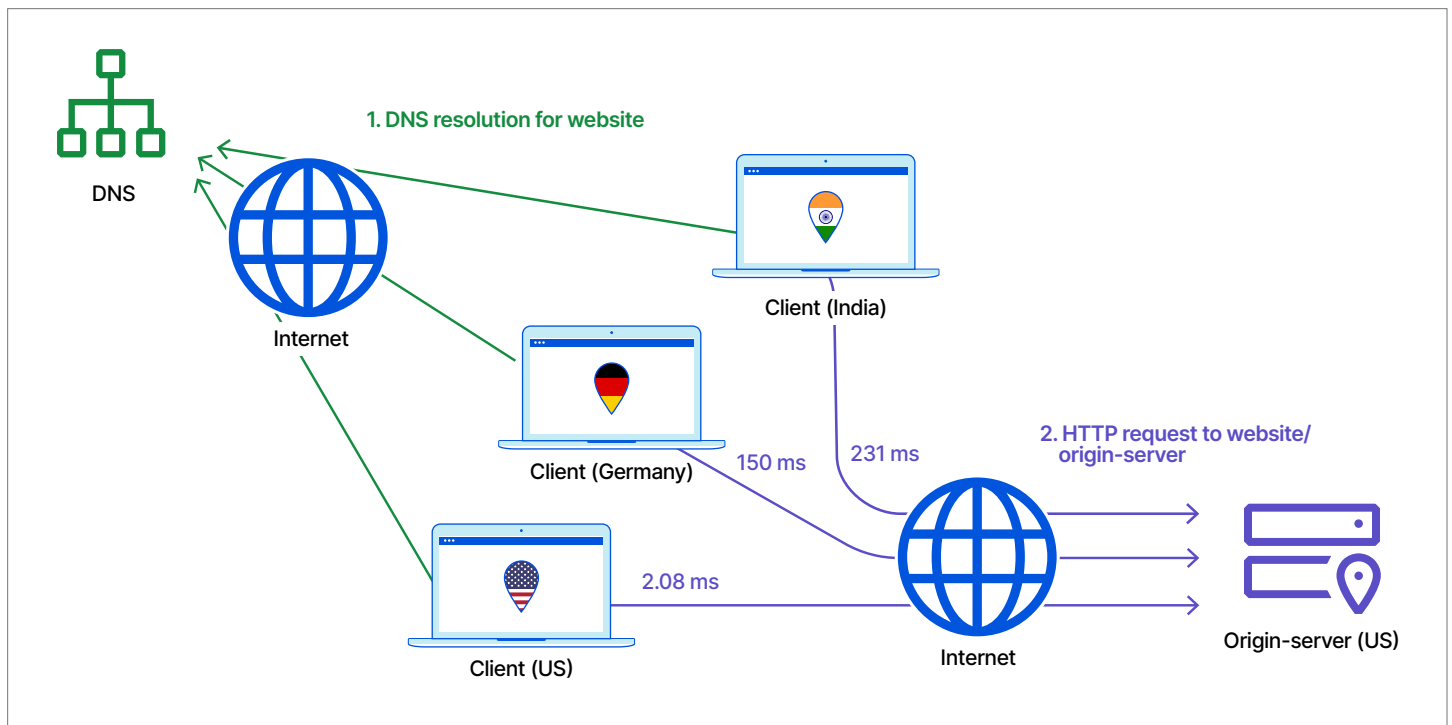


Figure 1: HTTP Request with no CDN

CLOUDFLARE CDN REFERENCE ARCHITECTURE

How a CDN tackles web application challenges

A CDN helps address the challenges customers face around latency, performance, availability, redundancy, security, and costs. [A CDN's core goal is to decrease latency and increase performance](#) for websites and applications by caching content as close as possible to end users or those accessing the content.

CDNs decrease latency and increase performance by having many data center locations across the globe that cache the content from the origin. The goal is to have content cached as close as possible to users, so content is cached at the edge of the CDN provider's network.

The impact this has:

- **Improved website load time**
Instead of every client making a request to the origin server, which could be located a considerable distance away, the request is routed to a local server that responds with cached content, thus decreasing latency and increasing overall performance. Regardless of where the origin server and clients are located, performance will be more consistent for all users, as the CDN will serve locally cached content when possible.
- **Increased content availability and redundancy**
Because every client request no longer needs to be sent to the origin server, CDNs provide not only performance benefits, but also availability and redundancy. Requests are load balanced over local servers with cached content; these servers respond to local requests, significantly decreasing overall load on the origin server. The origin server only is contacted when needed (when content is not cached or for dynamic non-cacheable content).
- **Improved website security**
A CDN acts as a reverse proxy and sits in front of origin servers. Thus it can provide enhanced security such as DDoS mitigation, improvements to security certificates, and other optimizations.
- **Reduced bandwidth costs**
Because CDNs use cached content to respond to requests, the number of requests sent to the origin server is reduced, thus also reducing associated bandwidth costs.

An important difference in some CDN implementations is how they route traffic to the respective local CDN nodes.

Routing requests to CDN nodes can be done via two different methods:

1. DNS unicast routing

In this method, recursive DNS queries redirect requests to CDN nodes; the client's DNS resolver forwards requests to the CDN's authoritative nameserver. CDNs based on DNS unicast routing are not ideal in that clients may be geographically dispersed from the DNS resolver. Decisions on closest-proximity CDN nodes are based on the client's DNS server instead of client's IP address.

Also, if any changes are needed for the DNS response, there is a dependency on DNS time to live (TTL) expiration.

Further, since DNS routing uses unicast addresses, traffic is routed directly to a specific node, creating possible concerns when there are traffic spikes, as in a DDoS attack.

Another challenge with DNS-based CDNs is that DNS is not very graceful upon failover. Typically a new session or application must be started for the DNS resolver with a different IP address to take over.

2. Anycast routing

The Cloudflare CDN, which is discussed in more detail in the next section, uses Anycast routing. Anycast allows for nodes on a network to have the same IP address. The same IP address is announced from multiple nodes in different locations, and client redirection is handled via the Internet's routing protocol, BGP.

Using an Anycast-based CDN has several advantages:

- Incoming traffic is routed to the nearest data center with the capacity to process the requests efficiently.
- Availability and redundancy is inherently provided. Since multiple nodes have the same IP address, if one node were to fail, requests are simply routed to another node in close proximity.
- Because Anycast distributes traffic across multiple data centers, it increases the overall surface area, thus preventing any one location from becoming overwhelmed with requests. For this reason, Anycast networks are very resilient to DDoS attacks.

CLOUDFLARE CDN REFERENCE ARCHITECTURE

Introducing the Cloudflare CDN

Cloudflare provides a Software as a Service (SaaS) model for CDN. With Cloudflare's SaaS model, customers benefit from the Cloudflare CDN without having to manage or maintain any infrastructure or software.

The benefits of the Cloudflare CDN can be attributed to the below two points, discussed in more detail in this section.

1. CDNs inherently increase performance by caching content on servers close to the user
2. The unique Cloudflare architecture and integrated ecosystem

Figure 2 shows a simplified view of the Cloudflare CDN. Clients are receiving their response back from a server on Cloudflare's global Anycast edge network closest to where the clients are located, thus drastically reducing the latency and RTT. The diagram depicts a consistent end-user experience regardless of the physical location of the clients and origin.

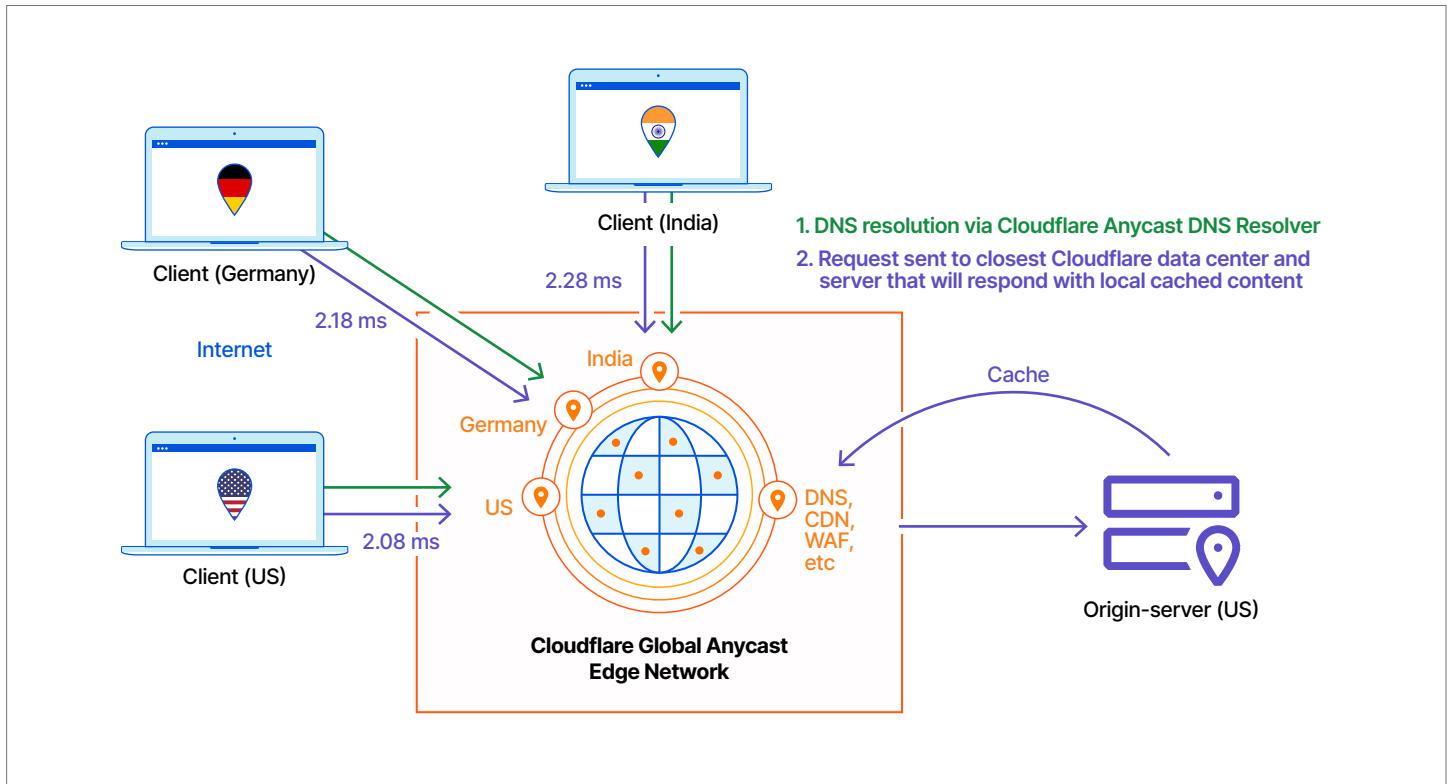


Figure 2: HTTP request to Cloudflare CDN with Anycast

CLLOUDFLARE CDN REFERENCE ARCHITECTURE

Cloudflare CDN architecture and design

Figure 3 is a view of the Cloudflare CDN on the global Anycast edge network. In addition to using Anycast for network performance and resiliency, the Cloudflare CDN leverages Argo Tiered Cache to deliver optimized results while saving costs for customers. Customers can also enable Argo Smart Routing to find the fastest network path to route requests to the origin server. These capabilities are discussed in detail in the remainder of this document.

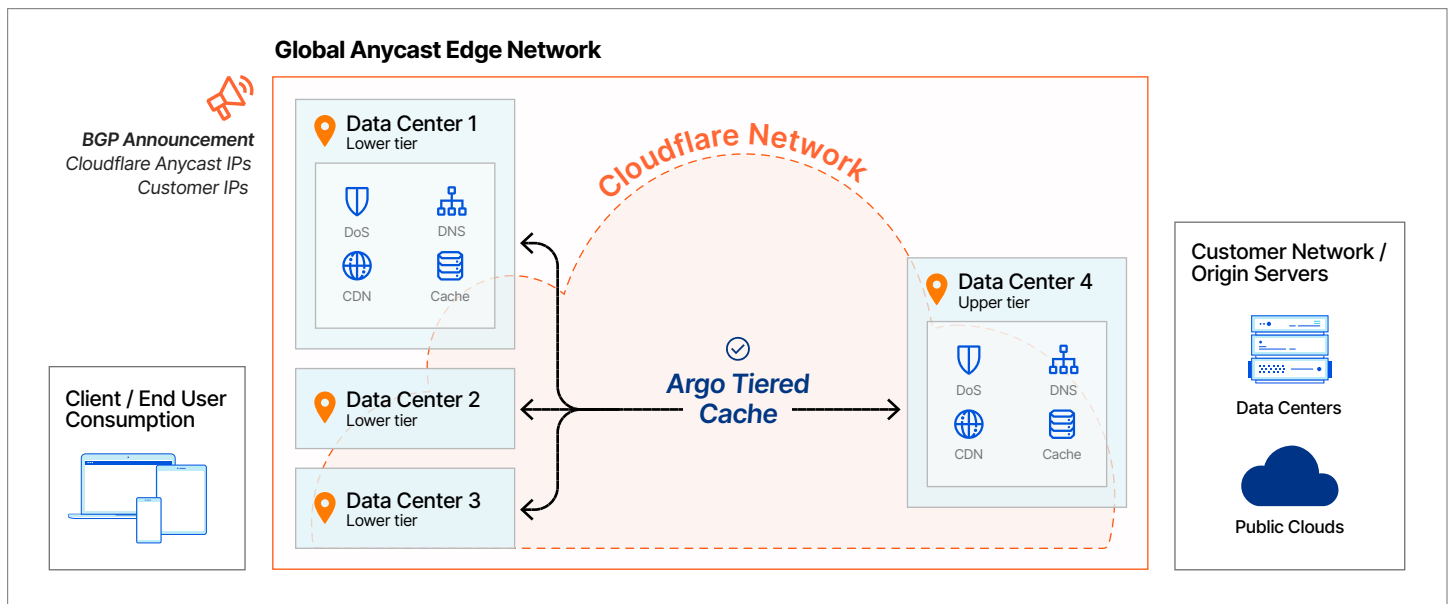


Figure 3: Cloudflare CDN with Argo Tiered Cache on global Anycast edge network

In the above diagram, there are a few important key points to understand about the Cloudflare CDN and the global Anycast edge network it resides on:

- An important differentiator is that Cloudflare utilizes one global network and runs every service on every server in every Cloudflare data center, thus providing end users the closest proximity to Cloudflare's services, with the highest scale, resiliency, and performance.
- Cloudflare is a reverse proxy, meaning it receives requests from clients and proxies the requests back to the customer's origin servers.

Thus, every request traverses through Cloudflare's network before reaching the customer's network.

Since Cloudflare has hardened and protected its infrastructure at the edge (ingress), all customers are consequently also protected from infrastructure-level and volumetric DDoS attacks. Requests and traffic must go through the protected Cloudflare network before reaching the customer's origin server.

- The Cloudflare CDN leverages the Cloudflare global Anycast edge network. Thus the incoming request is routed to and answered by the node closest to the user (eyeball).
- The inherent benefits of Anycast are decreased latency, network resiliency, higher availability, and increased security due to larger surface area for absorbing both legitimate traffic loads and DDoS attacks.

CLOUDFLARE CDN REFERENCE ARCHITECTURE

Cloudflare CDN architecture and design (continued)

Cloudflare's global Anycast edge network spans more than 250 cities across 100+ countries, reaching 95% of the world's Internet-connected population within 50 milliseconds while providing 100 Tbps of network capacity and DDoS protection capability.

- Edge nodes within the Cloudflare network cache content from the origin server and are able to respond to requests via a cached copy. Cloudflare also provides DNS, DDoS protection, WAF, and other performance, reliability, and security services using the same edge architecture.

- Argo uses optimized routing and caching technology across the Cloudflare network to deliver responses to users more quickly, reliably, and securely. Argo includes Smart Routing and Tiered Cache. Cloudflare leverages Argo to provide an enhanced CDN solution.

Argo Tiered Cache

Once a site is onboarded, standard caching is configured by default. With standard caching, each data center acts as a direct reverse proxy for the origin servers. A cache miss in any data center results in a request being sent to the origin server from the ingress data center.

Although standard caching works, it is not the most optimal design — cached content closer to the client may already exist in other Cloudflare data centers, and origin servers are sometimes unnecessarily overloaded as a result. Thus, it is best to enable Argo Tiered Cache, which is included with every Cloudflare plan. With Argo Tiered Cache, certain data centers are reverse proxies to the origin for other data centers, resulting in more cache hits and faster response times.

Argo Tiered Cache leverages the scale of Cloudflare's network to minimize requests to customer origins. When a request comes into a Cloudflare data center, if the requested content is not locally cached, other Cloudflare data centers are checked for the cached content.

Cloudflare data centers have shorter distances and faster paths between them than the connections between data centers and customer origin servers, optimizing the response to the client with a significant improvement in cache hit ratio. The Cloudflare CDN leverages Argo Smart Routing data to determine the best upper tier data centers to use for Argo Tiered Cache. Argo Smart Routing can also be enabled as an add-on to provide the fastest paths between data centers and origin servers for cache misses and other types of dynamic traffic.

The Cloudflare CDN allows customers to configure tiered caching. Note that depending on the Cloudflare plan, different topologies are available for Argo Tiered Cache. By default, tiered caching is disabled and can be enabled under the caching tab of the main menu.

CLLOUDFLARE CDN REFERENCE ARCHITECTURE

Argo Tiered Cache Topologies

The different cache topologies allow customers to control how Cloudflare interacts with origin servers to help ensure higher cache hit ratios, fewer origin connections, and reduced latency.

Argo Tiered Cache Topologies		
Smart Tiered Cache Topology (All plans)	Generic Global Tiered Topology (Enterprise Only)	Custom Tiered Cache Topology (Enterprise Only)
<ul style="list-style-type: none"> Recommended for most deployments. It is the default configuration once Tiered Cache is enabled. Ideal for customers who want to leverage CDN for performance but minimize requests to origin servers and bandwidth utilization between Cloudflare and origin servers. Cloudflare will dynamically find the single best upper tier for an origin using Argo performance and routing data. 	<ul style="list-style-type: none"> Recommended for those who have high traffic that is spread across the globe and desire the highest cache usage and best performance possible. Generic Global Tiered Topology balances between cache efficiency and latency. Instructs Cloudflare to use all Tier 1 data centers as upper tiers. 	<ul style="list-style-type: none"> Recommended for customers who have additional data on their user base and have specific geographic regions they would like to focus on. Custom Tiered Cache Topology allows customers to set a custom topology that fits specific needs (ex: upper tiers in specific geographic locations serving more customers). Engage with a Customer Success Manager (CSM) to build a custom topology.

CLOUDFLARE CDN REFERENCE ARCHITECTURE

Traffic flow: Argo Tiered Cache, Smart Tiered Cache Topology

In Figure 4, Argo Tiered Caching is enabled with Smart Tiered Cache Topology. The diagram depicts two separate traffic flows, summarized below. The first traffic flow (Client 1 in green) is a request from a client that comes into Data Center 1. The second traffic flow (Client 2 in purple) is a subsequent request for the same resource into a different data center, Data Center 2.

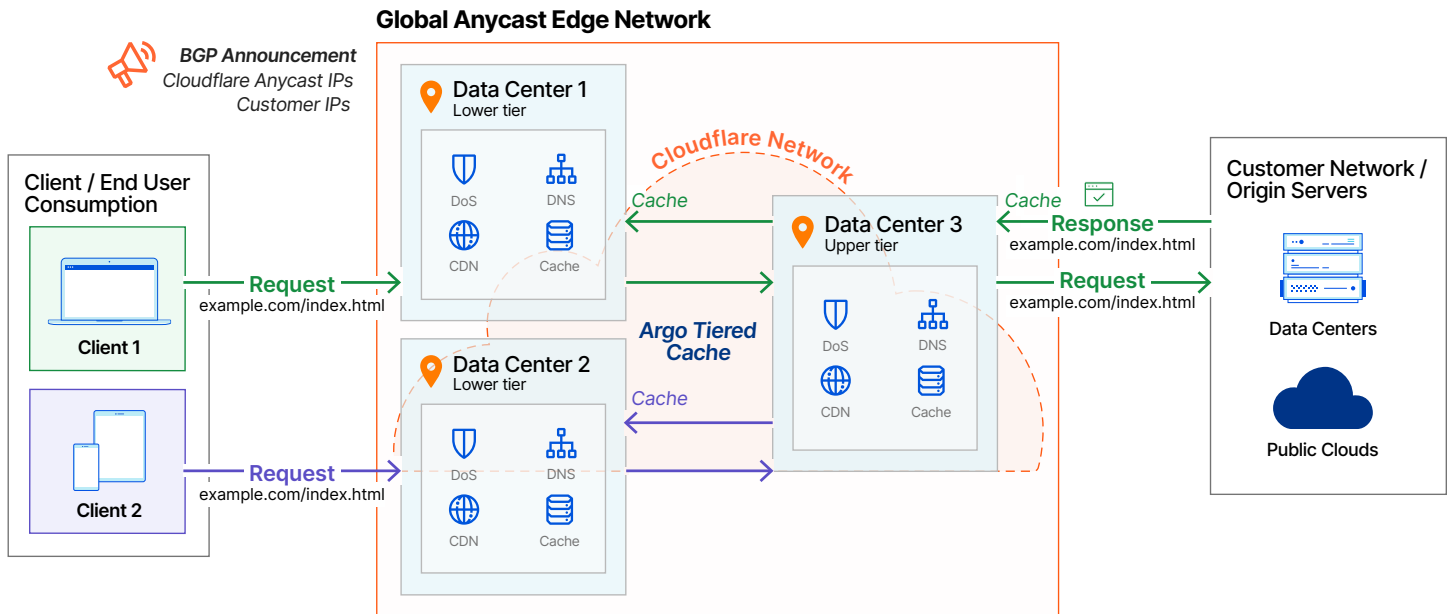
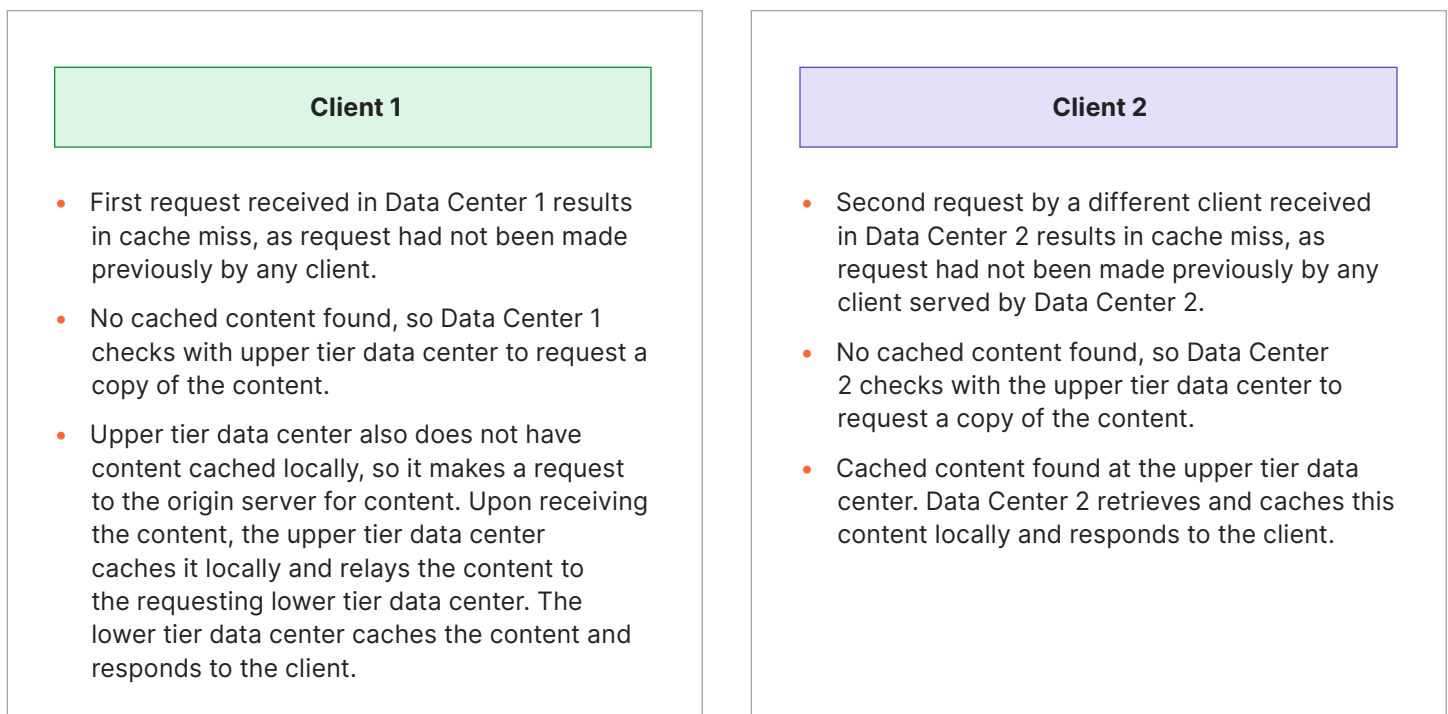


Figure 4: HTTP requests and traffic flow through Cloudflare CDN



CLOUDFLARE CDN REFERENCE ARCHITECTURE

Traffic flow: Argo Tiered Cache, Smart Tiered Cache Topology (Continued)

In Figure 4, Client 1 traffic flow displays the traffic flow when a client request is received by a data center closest to the client, Data Center 1. Since there is nothing locally cached on the ingress data center and tiered caching is enabled, a request is sent to the upper tier data center to request a copy of the content to cache.

Because the upper tier data center also does not have the content cached, it sends the request to the origin server, caches the received content upon response, and responds to the lower tier data center with the cached content. The lower tier data center caches the content and responds to the client.

Argo Smart Routing

Argo Smart Routing is a service that finds optimized routes across the Cloudflare network to deliver responses to users more quickly. As discussed earlier, Cloudflare CDN leverages Argo Smart Routing to determine the best upper tier data centers for Argo Tiered Cache.

In addition, Argo Smart Routing can be enabled to ensure the fastest paths over the Cloudflare network are taken between upper tier data centers and origin servers at all times. Without Argo Smart Routing, communication between upper tier data centers to origin servers are still intelligently routed around problems on the Internet to ensure origin reachability.

Notice that when a new request for the same content is made to another data center (Client 2 traffic flow), Data Center 2, the content is not locally cached; however, the content is retrieved from the upper tier data center, where it was cached from the first request for the same content.

With the upper tier data center returning the cached content for the second request, the trip to the origin server is prevented, resulting in higher cache hit ratios, faster response times, saved bandwidth cost between the Cloudflare network and the origin server, and reduced load on the origin server responding to requests.

Argo Smart Routing accelerates traffic by taking into account real-time data and network intelligence from routing over 28 million HTTP requests per second; it ensures the fastest and most reliable network paths are traversed over the Cloudflare network to the origin server. On average, Argo Smart Routing accounts for 30% faster performance on web assets.

CLOUDFLARE CDN REFERENCE ARCHITECTURE

Traffic Flow: Argo Tiered Cache, Smart Tiered Cache Topology with Argo Smart Routing

Figure 5 details the traffic flow when Argo Tiered Cache and Argo Smart Routing are not enabled. The request comes into the closest data center, and, because content is not locally cached and Argo Tiered Cache is not enabled, the request is sent directly to the origin server for the content. Also, since Argo Smart Routing is not enabled, a reliable, but perhaps not the fastest, path is taken when communicating with the origin server.

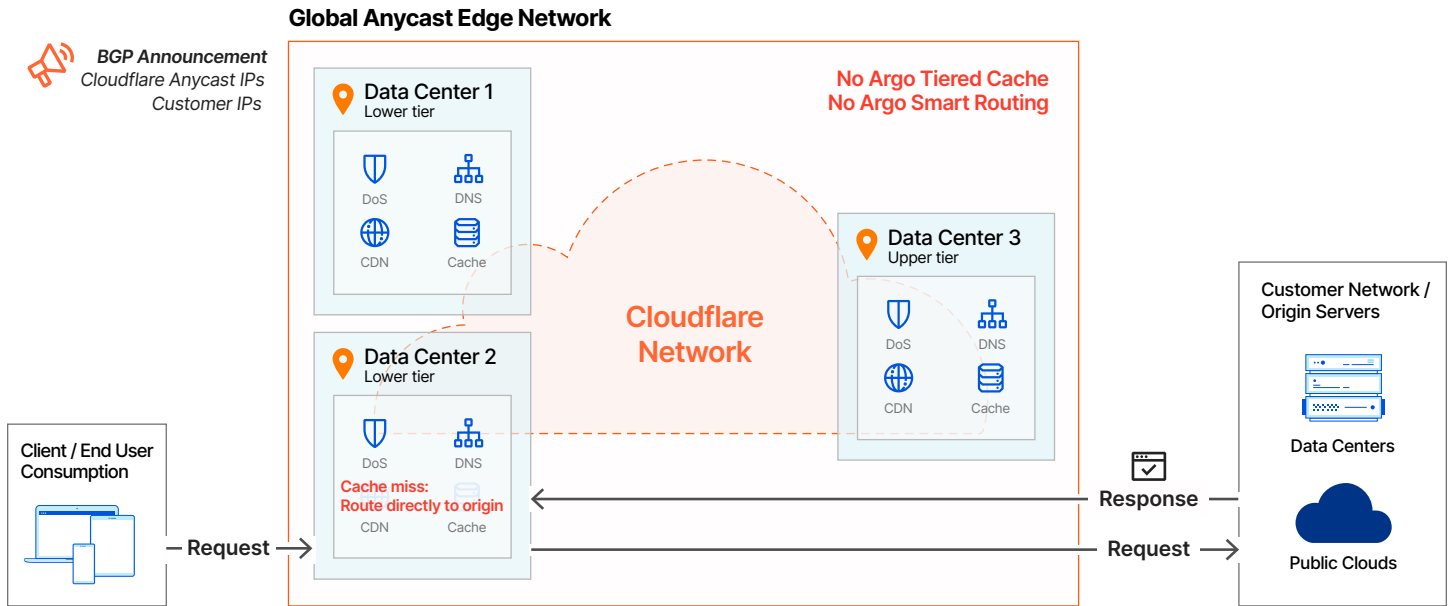


Figure 5: Cloudflare CDN without Argo Tiered Cache and Argo Smart Routing

CLOUDFLARE CDN REFERENCE ARCHITECTURE

Traffic Flow: Argo Tiered Cache, Smart Tiered Cache Topology with Argo Smart Routing (continued)

Figure 6 articulates the traffic flow with both Argo Tiered Cache and Argo Smart Routing enabled.

In Figure 6, when a request is received by Data Center 1 and there is a cache miss, the cache of the upper tier data center, Data Center 3, is checked. If the cached content is not found at the upper tier data center, with Argo Smart Routing enabled, the request is sent on the fastest path from the upper tier data center to the origin.

The fastest path is determined by the Argo network intelligence capabilities, which take into account real-time network data such as congestion, latency, and RTT.

With the Cloudflare CDN, Argo Smart Routing is used when:

1. There is a cache miss and the request needs to be sent to the origin server to retrieve the content,
2. There is a request for non-cacheable content, such as dynamic content (ex: APIs), and the request must go to the origin server.

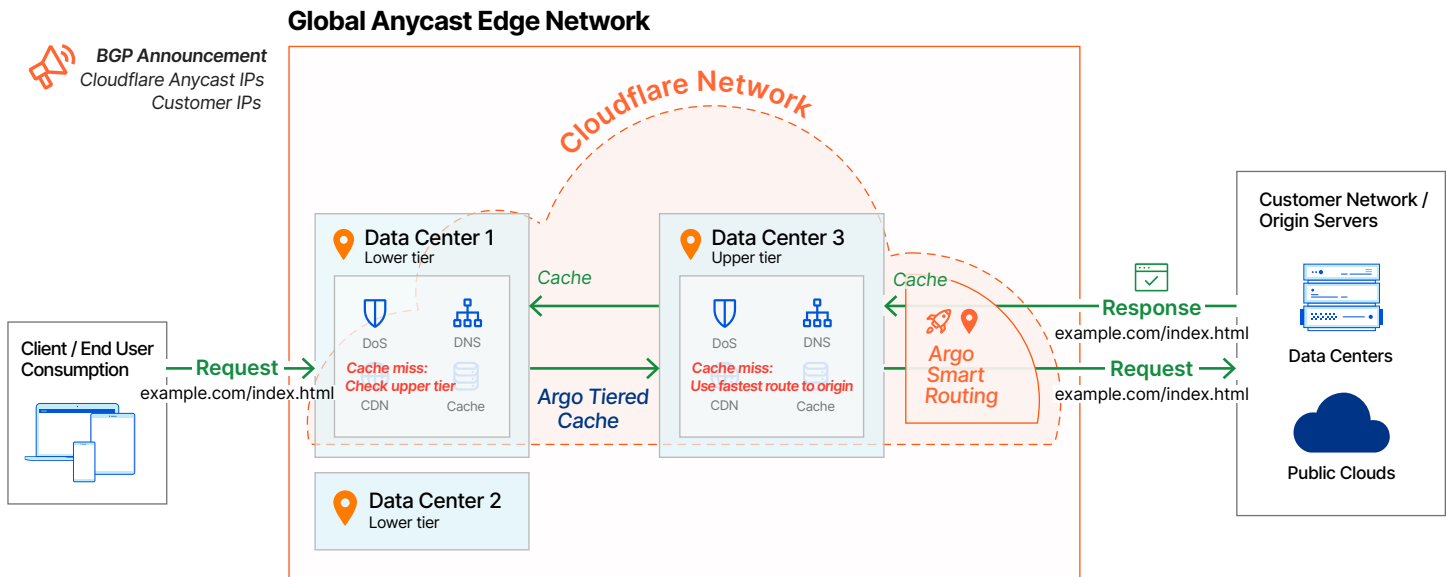


Figure 6: Cloudflare CDN with Argo Tiered Cache and Argo Smart Routing enabled

CLOUDFLARE CDN REFERENCE ARCHITECTURE

Summary

To summarize, the Cloudflare CDN is SaaS that helps address the challenges customers face around latency, performance, availability, redundancy, security, and costs. The Cloudflare CDN leverages Cloudflare's global Anycast edge network and Argo Tiered Cache to deliver optimized results while saving costs for customers. Customers can also enable Argo Smart Routing to ensure the fastest network path is used to route requests to the origin server.

WHITEPAPER

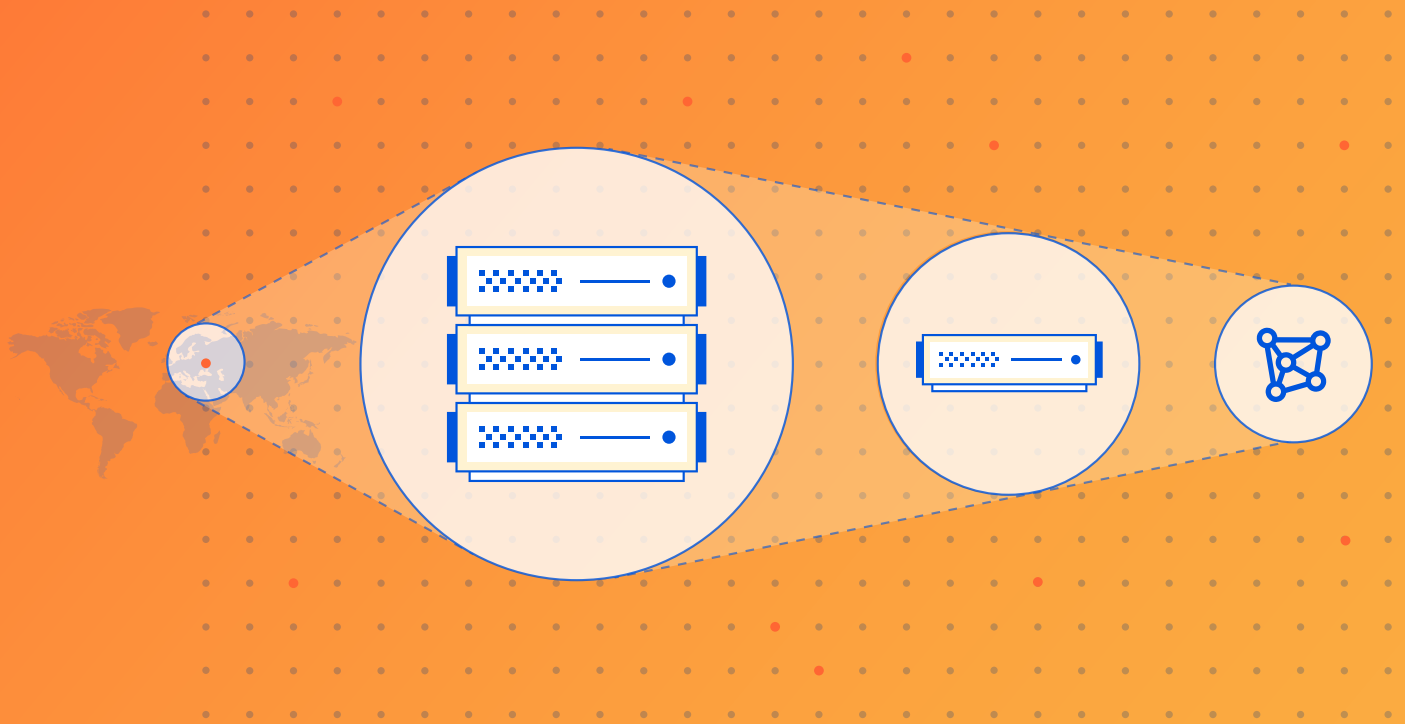


© 2022 Cloudflare Inc. All rights reserved. The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.



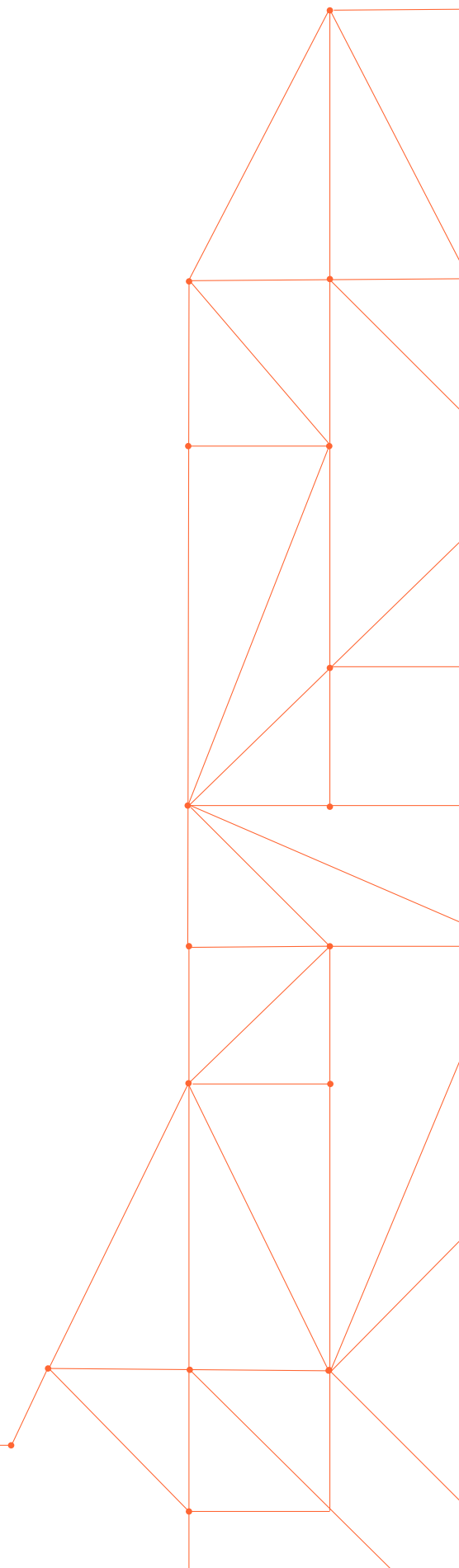
WHITEPAPER

DNS and the Threat of DDoS



Content

- 03** Executive Summary
- 04** Large, growing attacks pose a new degree of threat to DNS
- 04** Massive IoT-based and server-based botnets
- 05** Overwhelming DNS servers: UDP floods
- 05** Exploiting how DNS works: DNS amplification
- 06** The impacts of large DDoS attacks on DNS resolvers and downstream victims
- 06** How to stop the coming threats targeting DNS infrastructure
- 06** Legacy DDoS mitigation via hardware vs. scalable mitigation via software
- 07** The future does not come in a box
- 08** How Cloudflare easily scales up DNS security
- 09** Winning the arms race and remaining resilient in the face of DDoS attacks
- 09** Protecting DNS from all kinds of attacks and exploitation
- 10** Takeaways
- 11** References

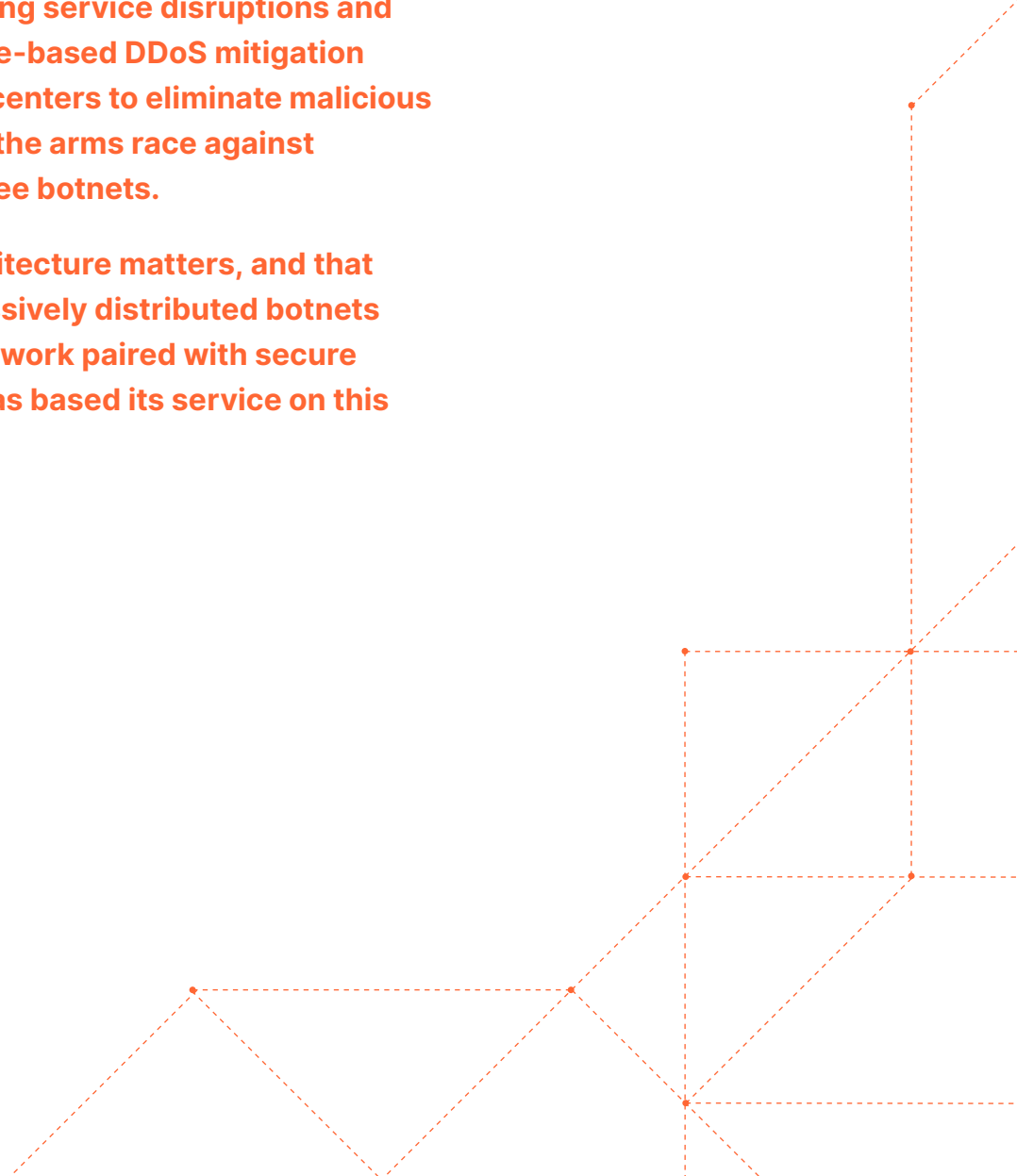


Executive Summary

The Domain Name System (DNS) was one of the major innovations that made the Internet possible. But today, massive botnets are being used to stage ever-larger cyber attacks using, and targeting, DNS infrastructure.

In recent years, attackers have been able to take down essential services and huge patches of the Internet using large distributed denial-of-service (DDoS) attacks against DNS, with a large number of high-profile sites and organizations experiencing service disruptions and outages. Traditional hardware-based DDoS mitigation services that use scrubbing centers to eliminate malicious traffic cannot scale to win in the arms race against distributed and essentially free botnets.

Cloudflare believes that architecture matters, and that the only solution against massively distributed botnets is a massively distributed network paired with secure DNS resolution. Cloudflare has based its service on this architectural approach.



Large, growing attacks pose a new degree of threat to DNS

On October 21, 2016, a massive and sustained distributed denial-of-service (DDoS) attack impacted huge parts of the Internet, interrupting or bringing down dozens of high-profile websites and services. The direct target of the attack was Dyn, a DNS service provider, which maps domain names to their Internet Protocol (IP) addresses so that traffic can be routed to a specific site. The attack took hours to mitigate.¹

But that was just the beginning of a growing wave of extremely large DDoS attacks. In the years since, attacks have increased in scale and scope, culminating in some of the biggest cyber attacks on record. AWS reported mitigating a massive DDoS attack in February of 2020. At its peak, this attack saw incoming traffic at a rate of 2.3 terabits per second (Tbps).² And In June 2022, Cloudflare mitigated a 26 million request per second DDoS attack — the largest HTTPS DDoS attack on record to that point.³

How are attackers able to scale up their attacks to these heights?

Massive IoT-based and server-based botnets

One major way that large attacks are generated is through taking over poorly protected Internet of Things (IoT) devices. The Mirai botnet is perhaps the highest-profile example of a network of IoT devices exploited for malicious purposes. The creators of Mirai compromised over 100,000 connected devices, such as home routers, smart home gadgets, security cameras, or video recorders, to create a huge botnet, which was used to launch the Dyn attack (among others) with potentially as much as 1.2 Tbps of traffic.

This massive botnet overwhelmed Dyn, which shut down DNS resolution for all the websites and applications relying on it.

“Assuming a device is publicly accessible, the chance of being hacked is probably 100 percent. The IPv4 address space just isn’t that big. You can now run a scan across that entire space in hours, especially if you have a big botnet. The scans for vulnerability are continuous, and if anything, have accelerated over the last couple of years.”

- Matthew Prince, CEO of Cloudflare

The botnet was created using a malware called Mirai. Mirai scans the Internet for devices that still have the factory-default username and password settings, making it easy to then infect it, log in, and take control of the device. The owner of the devices will not notice that the device was compromised, other than occasional sluggish performance.

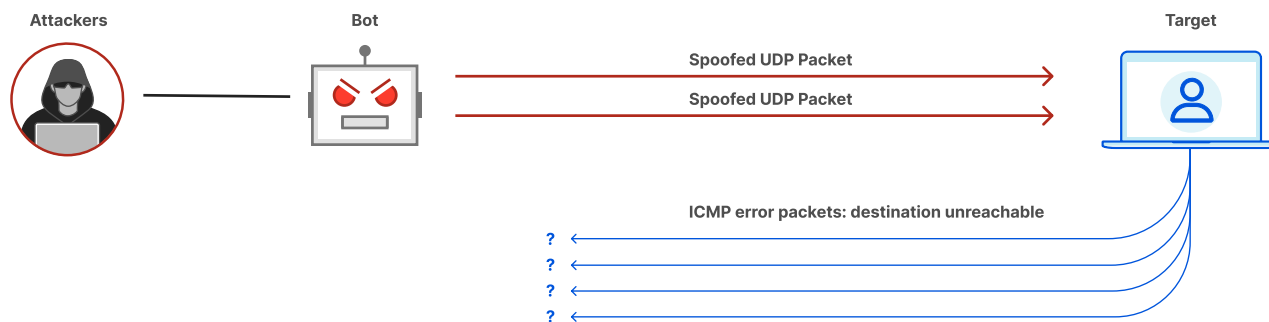
The Mirai botnet, which is still a threat today, is far from the only one that is actively used in DDoS attacks:

- The **Meris botnet** was first detected in June 2021. While researchers identified at least 30,000 bots within the botnet, the actual number of bots is believed to be much higher.⁴
- The **Mantis botnet** uses hijacked virtual machines and powerful servers instead of IoT devices. This means that each bot has far more computational resources than the devices in Mirai or Meris. The botnet is able to create massive DDoS attacks, as large as 26 million requests per second in some cases.⁵

The two most common methods for exploiting how DNS works are DNS amplification (or “reflection”) attacks and UDP flood attacks.

Overwhelming DNS servers: UDP floods

UDP flood attacks send a large number of UDP packets to a targeted server with the aim of overwhelming that device's ability to process and respond. The firewall protecting the targeted server can also become exhausted as a result of UDP flooding, resulting in a denial-of-service to legitimate traffic.



Such attacks are particularly relevant to DNS resolvers, since all DNS traffic is generally sent over UDP (not TCP is only used in some specific use cases like zone transfers). Because UDP requires no handshake to open a connection, large volumes of junk UDP packets can be sent to the target, which will then do its best to respond to each one. (The Mirai attack on Dyn, for example, was a UDP flood attack — when such attacks target DNS, they may be called a “DNS flood”.)

A UDP flood works primarily by exploiting the steps that a server takes when it responds to a UDP packet sent to one of its ports. If no programs are receiving packets at that port, the server responds with a ICMP (ping) packet to inform the sender that the destination was unreachable. As each new UDP packet is received by the server, it goes through steps in order to process the request, utilizing server resources in the process. As a result of the targeted server utilizing resources to check and then respond to each received UDP packet, the target's resources can become quickly exhausted when a large flood of UDP packets are received.

Exploiting how DNS works: DNS amplification

In addition to targeting DNS service providers directly, attackers can also weaponize their infrastructure and use the way DNS works to conduct crippling DDoS attacks to target others.

DNS amplification attacks leverage the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic. Instead of targeting the victim directly, each bot in the attack sends requests to open DNS resolvers with a spoofed IP address, which has been changed to the real source IP address of the targeted victim. The target then receives a response from the DNS resolvers.

The attacker structures the request in a way that generates as large a response from the DNS resolvers as possible. As a result, the target receives an amplification of the attacker's initial traffic. The Cybersecurity & Infrastructure Security Agency (CISA) estimates that DNS



amplification attacks can allow an attacker to send traffic up to 54 times the bandwidth of the spoofed packets they sent.⁶

DNS amplification was a crucial piece of the 2013 attack that knocked Spamhaus offline,⁷ and has been used in many other attacks in the wild as well.

While DNS resolvers are not directly responsible for these attacks, such exploitation of their systems can and should be prevented. Organizations with self-hosted DNS may also find their system working against them to take down their internal networks.

The impacts of large DDoS attacks on DNS resolvers and downstream victims

Organizations that have experienced DDoS attacks are well aware of their far-reaching negative impacts, which include downtime, lost business, reputational damage, and heavy financial burdens. One source found that on average, the total cost of a DDoS attack for enterprises was \$2 million, and the cost of a DDoS attack for small and medium-sized businesses was \$120,000. The cost of reacting to a DDoS attack could reach \$2.3 million for enterprises (as measured in 2017).⁸

Attacks directly on DNS providers can have even more far-reaching impacts for both the organizations that rely on them and the providers themselves: if their DNS goes down, organizations may look for a new provider.

Websites and applications are not the only targets of DDoS attacks. Attackers often target on-premise networks as well. Organizations with self-hosted DNS can be crippled while the attack goes on, with client devices unable to load needed resources. Such an attack can severely hinder an organization's operations, or stop them altogether.

How to stop the coming threats targeting DNS infrastructure

Ultimately only the right architecture can stop DDoS attacks that are growing in size with each passing year.

Legacy DDoS mitigation via hardware vs. scalable mitigation via software

Traditionally, the way to stop an attack was to buy or build a big box and use it to filter incoming traffic. Most legacy DDoS mitigation service vendors used hardware from companies like Cisco, Arbor Networks, and Radware clustered together into "scrubbing centers."

There were tricks to get these behemoth mitigation boxes to work together, but it was awkward. Physical limits on the number of packets a single box could absorb became the effective limit on the total volume that could be mitigated by a service provider. In very large DDoS attack situations, most of the attack traffic never reached the scrubbing center because, with only a few locations, upstream ISPs become the bottleneck.

The expense of the equipment meant that it was not cost effective to distribute scrubbing hardware broadly. It was typical for legacy DDoS vendors to only provision their service when a customer came under attack; it never made sense to have capacity beyond a certain margin over the largest attack previously seen.

It seemed rational to assume that any investment beyond that was a waste. But that assumption is proving ultimately fatal to this traditional model.

The future does not come in a box

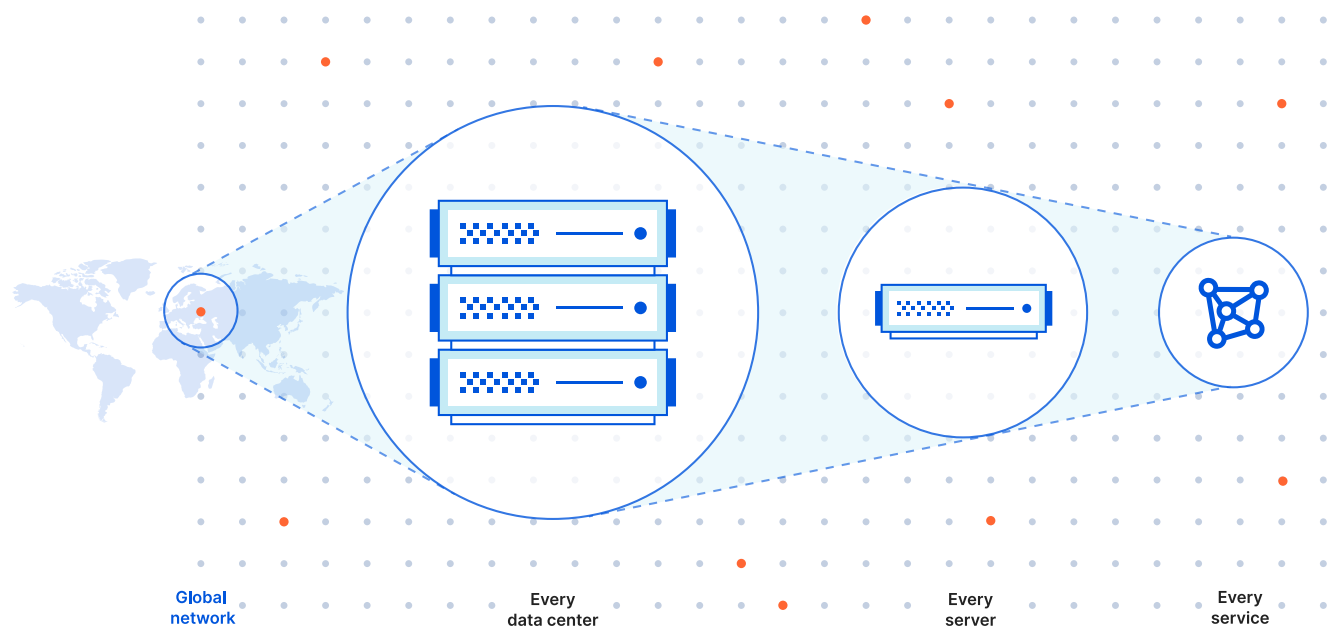
Instead of investing in hardware boxes for DDoS mitigation, from its earliest days Cloudflare started with a very simple architecture. Cloudflare's first racks had only three components: router, switch, server. Today the rack is even simpler, often dropping the router entirely and using switches that can also handle enough of the routing table to route packets across the geographic region the data center serves.

Rather than using load balancers or dedicated mitigation hardware, which could become bottlenecks in an attack, Cloudflare wrote software

that uses Border Gateway Protocol (BGP), the fundamental routing protocol of the Internet, to distribute load geographically, and within each data center in the network. Every server in every rack is able to answer every type of request. Cloudflare's software dynamically allocates traffic load based on what is needed for a particular customer at a particular time — meaning, Cloudflare automatically spreads load across literally tens of thousands of servers during large attacks.

It also means that Cloudflare can cost-effectively continue to invest in its network. For example, if a city needs 10% more capacity, Cloudflare can ship 10% more servers there, rather than having to make the step-function decision of whether to buy or build another scrubbing box.

Since every core, in every server, in every data center can help mitigate attacks, each new data center Cloudflare brings online makes the service better and more capable of stopping attacks nearer to the source. In other words, the solution to massively distributed botnets is a massively distributed network. This is how the Internet was meant to work: distributed strength, not focused brawn within a few scrubbing locations.



How Cloudflare easily scales up DNS security

But not only does Cloudflare use a distributed network to block and absorb malicious traffic efficiently, Cloudflare also provides authoritative DNS and DNS resolution from all of these locations. Serving DNS responses from any data center means DNS queries are resolved with minimal latency. It also means Cloudflare's DNS benefits from the entire network's capacity and distributed nature.

The Cloudflare network's efficient use of resources comes with operating savings as well as capital savings. Because Cloudflare uses the same equipment and networks to provide all of its functionality, Cloudflare rarely has any additional bandwidth costs associated with stopping an attack or providing any other service.

As Cloudflare's functionalities continue to expand, the capacity to stop attacks increases proportionately. Cloudflare can provide DDoS mitigation at a fixed cost to customers, regardless of the size of the attack, because attacks do not increase the largest of Cloudflare's unit costs.

This vast, distributed network of servers that all have the same capabilities also makes it simple for Cloudflare to offer functionalities at a massive scale and with minimal latency. One of the most core services is authoritative and secondary DNS; Cloudflare is the fastest DNS resolver in the world.⁹



The Cloudflare global Anycast network allows DNS resolution at the network edge in each data center across 275+ cities, resulting in unparalleled redundancy and 100% uptime. As Cloudflare's network capacity is well able to absorb DDoS attacks, the result is DNS that is resilient in the face of attacks of any size and type.

Winning the arms race and remaining resilient in the face of DDoS attacks

- Cloudflare's network capacity as of Q4 2022: **172 Tbps** (and growing)
- The largest DDoS attack ever recorded: less than **2.5 Tbps**

The size of DDoS attacks may continue to grow rapidly, even exponentially, in the coming years. But Cloudflare is positioned to continue winning the arms race for decades to come.

Cloudflare is the only provider that was designed from the beginning to mitigate large-scale DDoS attacks. Just as DDoS attacks are by their very nature distributed, Cloudflare's DDoS mitigation system is also distributed across its massive global network.

Against most legacy service providers, attackers have an advantage: providers' costs are high because they have to buy expensive boxes and bandwidth, while attackers' costs are low because they use an overwhelming number of hacked devices and generate an asymmetrical amount of traffic against their targets. That is why Cloudflare's secret sauce is the software that allocates the load across Cloudflare's massively distributed network of commodity hardware.

Protecting DNS from all kinds of attacks and exploitation

Cloudflare processes approximately 22.6 million DNS queries per second (both authoritative and resolution requests), as of Q4 2022 — all while mitigating growing DDoS attacks. Cloudflare DNS remains resilient against DDoS and bot attacks of any scale, from the large DDoS attacks of today to DNS water torture and other exploits.

For DNS service providers and organizations that host their own DNS infrastructure, the Cloudflare DNS Firewall provides a solution that not only helps them protect their infrastructure and users from large scale DDoS attacks, but also improves their performance by caching DNS records and responding on their behalf.



By natively integrating with DDoS mitigation, Cloudflare's DNS and DNS Firewall solutions ensure that your applications are always protected and available, even when facing some of the largest DDoS attacks on record.

Takeaways

Cloudflare continues to expand, adding more cities and countries to its network regularly. Cloudflare remains ever-vigilant for new attacks, but is confident that its architecture is ultimately the right way to stop whatever comes next. Start partnering with the network that's built to stop attacks on DNS both now and in the years to come:

- Protect yourself against all DDoS attacks, including large botnet-based DDoS attacks as well as amplification attacks, by setting up Cloudflare
- Keep your DNS up and running despite attacks by relying on Cloudflare as your authoritative DNS provider
- Protect your DNS infrastructure and potential DDoS victims by using Cloudflare's DNS Firewall to rate limit and deflect attacks

The setup is very simple and usually takes less than 5 minute to get up and running. See the plans, ranging from Free to Enterprise, at [cloudflare.com/plans](https://www.cloudflare.com/plans).

To learn more about Cloudflare's solutions, visit:

Cloudflare DNS <https://www.cloudflare.com/dns/>

Cloudflare DDoS Mitigation [cloudflare.com/ddos](https://www.cloudflare.com/ddos)

Cloudflare DNS Firewall <https://www.cloudflare.com/dns/dns-firewall/>



References

1. "DDoS Attack Against Dyn Managed DNS." Dyn Status Updates, 21 October 2016, <https://www.dynstatus.com/incidents/nlr4yrr162t8>. Accessed 3 October 2022.
2. Cimpanu, Catalin. "AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever." ZDNET, 17 June 2020, <https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/>. Accessed 3 October 2022.
3. Yoachimik, Omer. "Cloudflare mitigates 26 million request per second DDoS attack." Cloudflare, 14 June 2022, <https://blog.cloudflare.com/26m-rps-ddos/>. Accessed 3 October 2022.
4. Ganti, Vivek and Omer Yoachimik. "A Brief History of the Meris Botnet." Cloudflare, 9 November 2021, <https://blog.cloudflare.com/meris-botnet/>. Accessed 3 October 2022.
5. Yoachimik, Omer. "Mantis - the most powerful botnet to date." Cloudflare, 14 July 2022, <https://blog.cloudflare.com/mantis-botnet/>. Accessed 3 October 2022.
6. "Alert (TA14-017A): UDP-Based Amplification Attacks." CISA, 18 December 2019, <https://www.cisa.gov/uscert/ncas/alerts/TA14-017A>. Accessed 24 October 2022.
7. Prince, Matthew. "The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)." Cloudflare, 20 March 2013, <https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/>. Accessed 24 October 2022.
8. Kobialka, Dan. "Kaspersky Lab Study: Average Cost of Enterprise DDoS Attack Totals \$2M." MSSP Alert, 25 February 2018, <https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m/>. Accessed 3 October 2022.
9. "DNS Performance Analytics and Comparison." DNSPerf, <https://www.dnsperf.com/>. Accessed 24 October 2022.



© 2022 Cloudflare Inc. All rights reserved. The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Cloudflare WAF

A WAF for modern application security

Application security challenges

Applications are as critical as ever to business, which is why they are relentlessly targeted by attackers, amounting to growing organizational security concerns.

Concerns range from remaining protected against emerging 0-day exploits, to detecting evasion attempts, to reducing risk of credential stuffing that leads to account takeover, to detecting data loss, even scanning for malware uploads to applications.

These concerns are coupled with the need to ensure application protections are part of a broader, unified security posture, that also protects APIs, stops bots, and reduces client-side risks. All of this must happen while not burdening teams with undue management headaches.



Cloudflare WAF

The Cloudflare web application firewall (WAF) is the cornerstone of our advanced application security portfolio that keeps applications secure and productive. Only the Cloudflare WAF provides full security visibility, delivers layered protections against OWASP attacks and emerging exploits, detects evasions and new attacks with machine learning, blocks account takeover, detects data loss, and more, while easily fitting into broader enterprise security workflows. Our powerful application security capabilities, such as API security and bot management, are fully integrated with our WAF, calling on the same powerful rules engine, delivered from one of the world's most connected global cloud platforms.



Attack visibility and detection

We offer differentiated security analytics to visualize all traffic, mitigated or not. It informs security teams of unknown attacks—and the protections they should create. It displays WAF attack scores, Bot scores, and content scanning analytics.



Fast protections for emerging attacks

With tens of thousands of vulnerabilities per year, our WAF quickly adds new managed rules to block exploits of newly-discovered (0-day) vulnerabilities. Our managed rules block exploits, complemented by machine learning-derived WAF attack scores, to detect evasions.

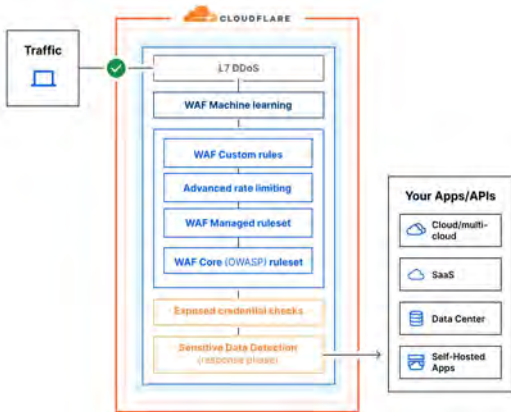


OWASP top ten threats

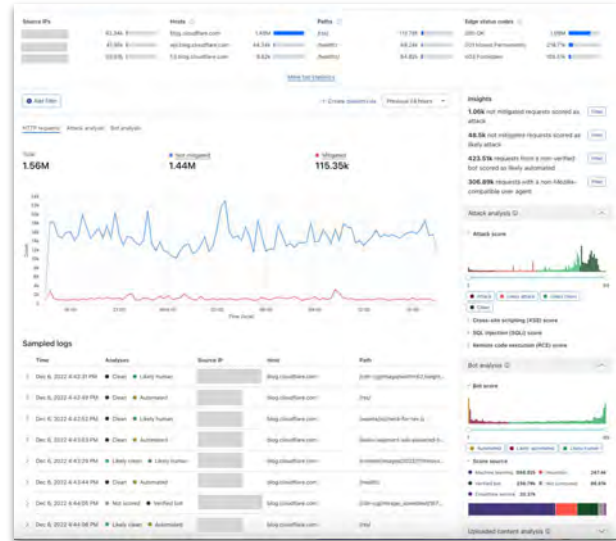
Attacks require layered defenses, including for known attack types in the OWASP top ten list. Our OWASP Core Ruleset is routinely updated and designed to work as a single entity to calculate a threat score and execute an action based on that score. This ruleset is configurable based on risk and security requirements.

Why Cloudflare Web Application Firewall

- Cloudflare protects more effectively.** We deliver more effective WAF security with layered protections:
 - Security analytics
 - Multiple managed rulesets
 - Custom rules
 - Machine learning detections
 - Sensitive data detection
 - Stolen credential checks
 - Advanced rate limiting
 - Malware upload scans
- Cloudflare responds faster.** We protect faster against exploits. For major vulnerabilities like Log4j, we had multiple managed rules in place a workday faster than other WAF vendors.
- Cloudflare fully integrates application security.** Our WAF is fully integrated with the rest of our application security portfolio, including API security and Bot management, all delivered in a single pass from one of the world's most connected global cloud platforms.



WAF security analytics



A WAF for enterprise security

SIEM-integrated, SOC-ready

With Cloudflare APIs and raw log integrations, it is easy to integrate with your SIEM or power your security operation center (SOC) with intelligence provided by Cloudflare.

DevSecOps made easier

Our out-of-the-box Terraform integration makes incorporating application security into DevOps approaches second nature.

Backed by Cloudforce One

Cloudflare application security receives threat intelligence from Cloudforce One, our threat operations team, blocking threats via new detections based on emerging intelligence and TTPs.

Cloudflare Leadership

Organizations gain a more effective application security posture with the Cloudflare global network as their enterprise security perimeter. The Cloudflare application security portfolio has received numerous accolades for its strength and breadth. Gartner named Cloudflare a leader in the 2022 Gartner® Magic Quadrant™ for Web Application and API Protection (WAAP). Cloudflare was recognized as a Leader in The Forrester Wave™ for WAF. Gartner also named the Cloudflare WAF a 2022 Customer's Choice. Frost & Sullivan recognized Cloudflare as an Innovation Leader in the 2020 Global Holistic Web Protection while IDC and Forrester named the company a 2021 DDoS leader.



REV:PMM-NOV 2022

Web Application Security

Layered protections from multiple WAF rulesets	<p>Stops malicious payloads in any request component with multiple rulesets:</p> <ol style="list-style-type: none"> 1. Cloudflare-managed rules 2. OWASP Core Ruleset 3. Custom rulesets to stop any attack. <p>New managed rules tested on vast amounts of traffic to ensure the fewest false positives.</p>
Updated rules for zero-day protections	Rules continuously updated by Cloudflare security teams for protection against novel attacks and zero-day vulnerability exploits before patches or updates are available.
Machine learning detections	Stop bypass attempts with machine learning models to complement layered rulesets. Four different attack score are available for rules: overall WAF attack score, XSS attack score, SQLi attack score, RCE attack score.
Platform-specific rule sets for major CMS and eCommerce platforms	Receive protection out of the box with no extra fees for platforms such as WordPress, Joomla, Plone, Drupal, Magento, IIS, etc.
Custom rule configuration	Choose from ALLOW, BLOCK, MANAGED CHALLENGE, JS CHALLENGE, SKIP, LOG, LEGACY CAPTCHA, CUSTOM RESPONSES when deploying rules or rulesets.
Advanced rate limiting	Stop abuse, DDoS, and brute-force attempts targeting applications and APIs by rate limiting individual IPs or by header attribute (e.g. key, cookie, token), ASN or country.
Threat intelligence feeds	Block connections from IPs of known open SOCKS proxies, VPNs, botnets, command and control servers, malware sources and anonymizers
Sensitive data detection	Detect responses containing sensitive data such as personally identifiable information, financial information, credit card numbers or secrets like API keys.
Exposed Credential Checks	Detect brute force attacks with stolen credentials before end user accounts are taken over.
Content upload scans	WAF content scanning will scan uploaded files for malware. Mitigation is done via WAF custom rules.
SSL/TLS	Fully offload and configure SSL traffic for your application.
Fewer false positives	New rules tested on vast amounts of traffic to ensure the fewest false positives.
gRPC and Websocket support	Proxy and secure traffic for gRPC and Websocket endpoints.
Customizable block pages	Customize block pages with appropriate detail for visitors.
Full integration with the broader Cloudflare product suite	Improve application performance, geo route traffic and leverage edge computing.

Visibility, Reporting, and Programmability

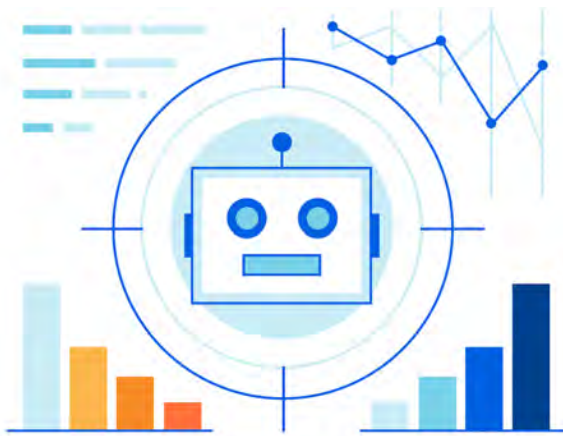
Security analytics	Visualization of all potential attacks, as scored by machine learning.
Real-time logging and raw log file access	Gain visibility to help you fine-tune the WAF; Conduct in-depth analysis covering all WAF requests
Payload logging	Log and encrypt malicious payloads for incident analysis
SIEM integrations	Push or pull logs directly into your existing SIEM.
Terraform integration	Incorporate application security into CI/CD workflows.

Management

Single console management	Streamlined management with a single console to deploy and manage global application security and performance.
Account-level management	Save time on WAF management via a single account-level WAF configuration for all domains.
High availability — with SLAs	100% uptime guarantee including financial penalties if SLAs are broken
No hardware, software or tuning required	Deploy with a simple change in DNS
PCI certification	Cloudflare possesses Level 1 service provider certification
FedRAMP Authorized	Our Cloudflare for Government suite, including application security, is FedRAMP authorized.

Cloudflare Bot Management

World-class bot protection from Cloudflare ensures uninterrupted business and lightning-fast web performance.



Cloudflare Bot Management ensures amazing web experiences for visitors. It stops bots from performing credential and credit card stuffing, inventory hoarding, and price scraping, while freeing up security teams to focus on other projects.

Bot Management is part of Cloudflare's application security portfolio. The portfolio also protects APIs, thwarts DDoS attacks, and monitors for malicious payloads and supply chain attacks.

Our application security products work closely with our performance suite, all delivered by the world's most connected global cloud platform.

The most innovative bot detection technology

Cloudflare Bot Management offers granular bot visibility and improves by the minute. Our network sees 25+ million HTTP requests per second; we use this data to conduct active machine learning and fingerprinting.



Detailed bot visibility

Bot Analytics delivers insight into bot patterns and abuse. Segment traffic by a number of different attributes, including bot score, detection engine, and other fields like IP address or user agent.



Layered bot defenses

We detect bots with five complementary detection engines: Heuristics, Machine Learning, Anomaly Detection, JavaScript Detections, and an allowlist for good bots. Cloudflare dynamically chooses the best engine for each request.



Intelligent challenge and response platform

Our response capabilities are dynamic: verify requests as legitimate while frustrating bad bots with fake content. Organizations decide when CAPTCHA or JavaScript challenges are presented, based on Bot Analytics.



Mobile API traffic support

Cloudflare draws on specialized API abuse detections to discern malicious bots from legitimate mobile traffic headed to APIs. We do this without a mobile SDK so as not to impose development burdens on organizations.

Bots never stop harming business

On any given day, bots make up roughly 50% of Internet traffic. Attackers automate bots to operate day and night — they carry out attacks that slow down web properties, or even knock them offline and undermine business.



Credential stuffing/account takeover

Credential stuffing attacks attempt log-ins using stolen credentials, under the assumption the same passwords are used across many sites. This can become account takeover.



Price and content scraping

Bots set up by competitors will scrape pricing data or even steal valuable content (used to undercut your business).



Inventory hoarding

Bots also hoard inventory, when they snap up low-inventory, highly sought-after merchandise in seconds, as soon as it is released, leaving real customers furious.



Content spam

Content and spam bots scrape contact information, create fake user accounts, and fill out marketing forms with dummy data.

World-class application security

The most precise protection

Always thread the needle between security and business with precise protections against bots and attacks. Cloudflare has been tested and tuned for the largest businesses.

Vast integrated capability

No slapdash acquisition code bases thrown together. Rather, integrated security, from a single console, constantly sharpening its threat stopping ability. Performance like CDN, DNS, and traffic acceleration is all built in.

Comprehensive security postures

We deliver full, enterprise-ready, cost-effective security capabilities. We'll never bleed you dry with limited base offerings requiring expensive add-ons or 3rd party marketplace integrations for a strong security posture.



Cloudflare Leadership

Organizations gain a more effective application security posture with the Cloudflare global network as their enterprise security perimeter. The Cloudflare application security portfolio has received numerous accolades for its strength and breadth. Gartner named the Cloudflare WAF a 2021 Customer's Choice. Frost & Sullivan recognized Cloudflare an Innovation Leader in Global Holistic Web Protection while IDC and Forrester named us as the DDoS leader.

Cloudflare Load Balancing

Product Presentation



CHALLENGES

Load Balancing in a heterogeneous environment can be complex



Sudden spikes in traffic lead to overloaded or unresponsive servers, resulting in slow response time and application downtime.



Operational costs and inflexibility of hardware load balancers restrict growth of business



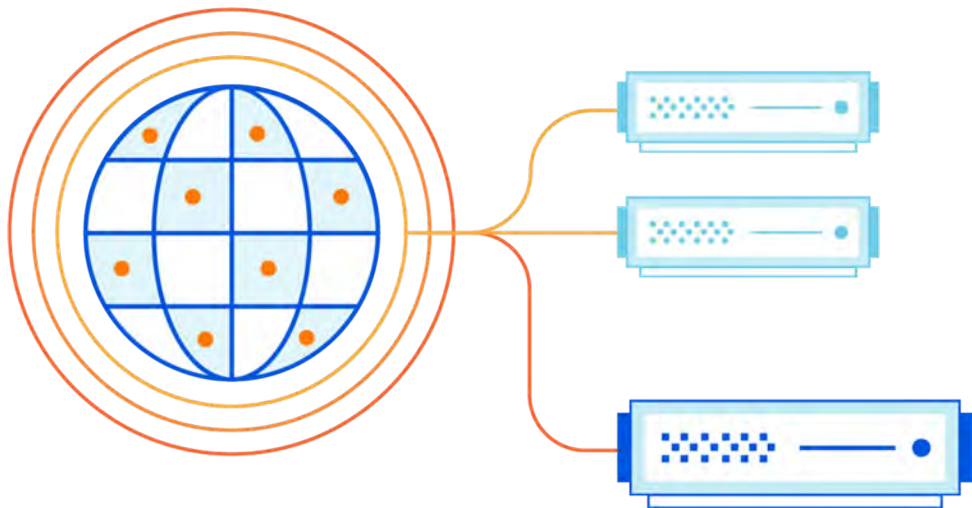
High complexity and cost of managing traffic in a multi-cloud or hybrid environment can be a huge overhead.



Lack of real-time visibility into traffic patterns and health of origins constraints optimal use of infrastructure.

CLOUDFLARE LOAD BALANCING

Cloudflare Load Balancing



**High availability
and performance
for your mission-
critical
applications.**

CLOUDFLARE LOAD BALANCING



Deliver an uninterrupted online experience

- Improve availability and performance by dynamically steering traffic to the most responsive pool.
- Deliver personalized experiences and comply with regulatory requirements such as GDPR by routing visitors to specific origins based on their location.
- Supports HTTP/S and TCP/UDP protocols.



Increase reliability with active health monitoring and fast failover

- Actively monitor origin health — make proactive decisions, not just reactive.
- Failover instantly from unhealthy origins. Requests proxied through Cloudflare get instantly re-routed — without waiting for TTLs to expire.
- No single point of failure. Load balance at every location



Get greater agility, visibility, and control

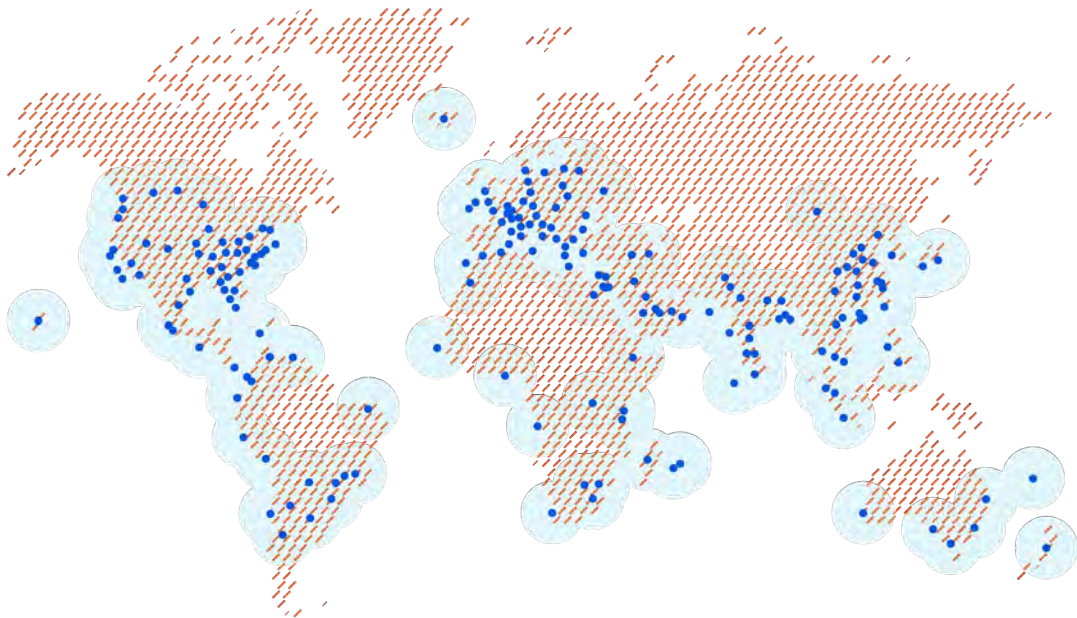
- *Agility:* Easy to set up. Scale without adding more metals
- *Visibility:* Get granular insights into your traffic and origin health
- *Control:* Unified control in a multi-cloud or hybrid environment

The Cloudflare Difference

THE CLOUDFLARE DIFFERENCE

Superior performance backed by our global anycast network

Note: map data as of
Jan 15, 2020



Load balance and perform health checks from every 400+ locations

Global propagation of changes in less than 5 seconds

No single point of failure

THE CLOUDFLARE DIFFERENCE

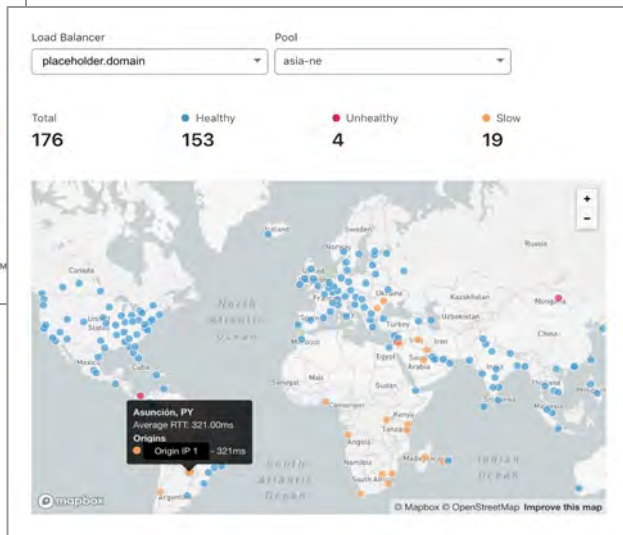
Unified control plane for complex environments



- **Improve agility** by creating rules at one place and deploying them across your infrastructure at the click of a button
- **Save costs** by avoiding costly vendor-lock ins
- **Better visibility** via centralized dashboard

THE CLOUDFLARE DIFFERENCE

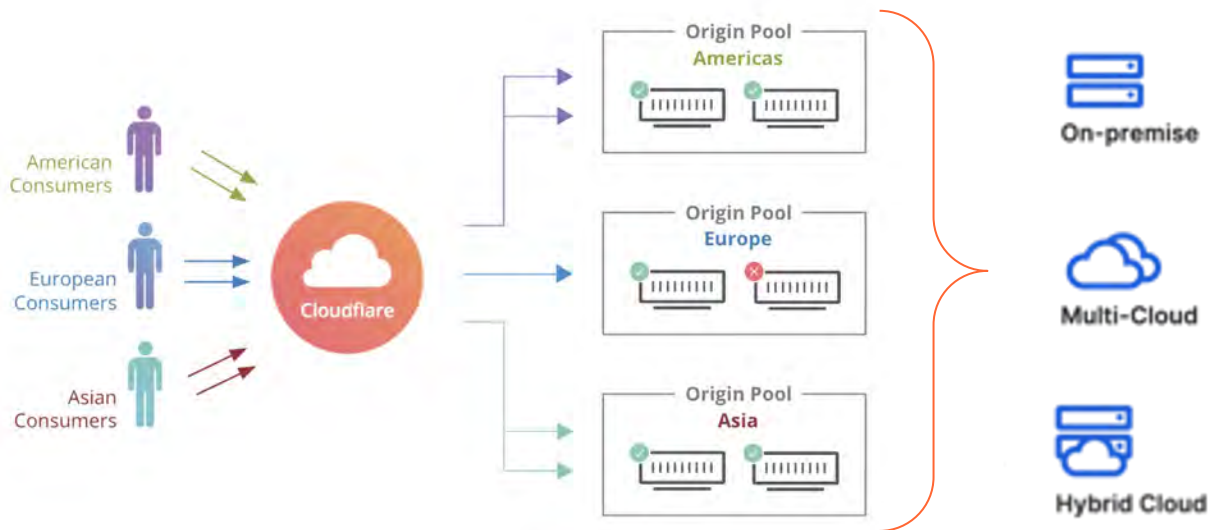
Know your traffic and origin health all the time



Not just raw logs. Cloudflare offers real-time visual representation of traffic patterns and origin health

THE CLOUDFLARE DIFFERENCE

Steer traffic the way you want it



Dynamic Steering

based on Round Trip Time (RTT)

Geo Steering

based on user's location

Weighted configuration

based on configurable weights

THE CLOUDFLARE DIFFERENCE

Simplify load balancing and make your life easy

Create Load Balancer

1. Hostnames 2. Origin Pools 3. Health Checks 4. Geotargeting 5. Settings

Add an Origin Pool

Pools are groups of origin servers ("endpoints") that Cloudflare will steer traffic to. Traffic is intelligently steered based on the health of each origin within the pool. Pools can be attached to a simple primary-secondary failover policy, or associated with a specific geographic region.

Origin Pools in this Load Balancer

The ordering of the pools in the load balancer determines the order in which pools in the load balancer will fail over. When the number of healthy origins within a pool goes below the configured threshold, Cloudflare will send traffic to the next available pool - e.g. traffic will always land on Pool #1 until it is marked unhealthy.

Order	Health	Name	No. of Origins	
1	Healthy	primary-pool	1 origin	Edit X

+ Add Pool

Pool Name: secondary-pool

Origin Name	Origin Address	
origin-server-2	52.74.74.5	X
server-2	2001:19f2:5::c0000000::c0000000	X

+ Add Origin

- Set up a fully-functioning load balancer **within minutes**
- **Easily add or remove servers** to the load balancers as traffic scales
- **Easily bind a user's session** to a specific origin

THE CLOUDFLARE DIFFERENCE

Build secure, scalable, and performant network applications through integration with *Cloudflare Spectrum*

Manage Monitors

Manage Monitors in all Load Balancers

Monitors actively probe the health of each of your origin servers from Cloudflare's data centers. An origin will be marked as 'unhealthy' when it fails to match the required settings below - e.g. returning 404 'Not Found' instead of a 200 'OK'.

[- Create a Monitor](#)

Type [?] Port [?]

Health Check Description (optional)

Advanced health check settings [?]

Interval [?]

Timeout [?] Retries [?]

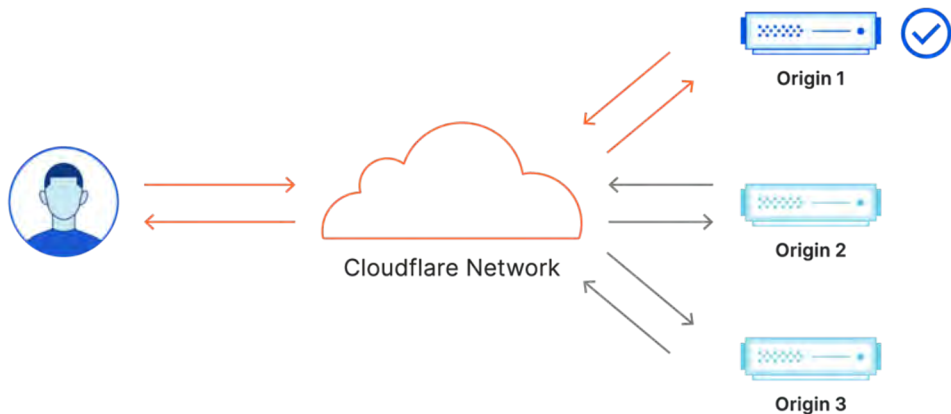
Cancel

Save

- Configure health checks to probe any TCP port.
- All steering modes are available for transport load balancing through Spectrum.
- Use the same Cloudflare dashboard or API to manage all your settings in one place.

THE CLOUDFLARE DIFFERENCE

Use session affinity to deliver an uninterrupted, seamless experience



- Bind a user's session to a specific origin, ensuring all requests during the session are sent to the same origin.
- Leverage origin drain functionality to disable origins or pools without affecting active customer sessions.

Customer Stories

CUSTOMER STORIES

Shopify

CHALLENGES

- For over one million businesses around the world, Shopify is the engine driving their online retail storefronts.
- Ensuring stellar performance and uptime is key — subpar shopping experience translates directly into lost revenue and erosion of consumer confidence.

SOLUTION

With Cloudflare Load Balancing, Shopify has granular control over how its traffic is distributed between its origin servers, with the added performance and accuracy benefits of making these decisions at the network edge. By using Cloudflare to broadcast its IP block, Shopify delivers faster, more reliable performance without needing merchants to modify their DNS settings.

VALUE

- Onboarded over one million domains and security certificates, with safeguards in place to ensure any changes could be quickly reverted.
- Saved large investments in infrastructure, expertise, and time by not building a large in-house network, and rather joining the Cloudflare's global network.



“Black Friday is one of the most important days for our merchants every year. With Cloudflare, we were able to handle the demand during this shopping season and deliver lightning-fast responses to shoppers globally.”

*— Charles Ng
Production Engineering
Manager*

cloudflare.com/case-studies/shopify-powering-the-biggest-shopping-weekend-of-the-year/

CUSTOMER STORIES

AutoTrader

CHALLENGES

- AutoTrader — the largest automobile classifieds service in the United Kingdom and Ireland wanted to transition from their current physical, data center-based hardware infrastructure to the next-generation — implemented and maintained in the cloud.
- They see over 55 million visits every month — this migration to the cloud was an undertaking with high stakes and little margin for error.

SOLUTION

With Cloudflare, AutoTrader replaced its entire stack that consisted of multiple differing technologies: F5 (load balancing / WAF), PowerDNS (on-premises DNS), Verisign DNS (key external domains), and Arbor (DDoS defence).

VALUE

- Realized major savings in overhead with no more hardware to maintain
- Attained a user experience that's vastly easier to navigate — managing DNS, performance, and security needs into a single unified interface.
- Extensive API support for automation tasks and the Cloudflare Workers to build out custom functionality.



“Not only is the product great in itself, but so are the people who work at Cloudflare — they really care, they’re passionate about the product. They want to help you succeed. It’s rare that you can find a company that you collaborate with where it feels like a real working partnership.”

*— Mark Bell
Systems Engineer*

cloudflare.com/case-studies/auto-trader-on-premises-cloud-migration/

CUSTOMER STORIES

Bitfinex

CHALLENGES

- Bitfinex is the world's largest and most advanced bitcoin trading platform. Hundreds of millions in transaction volume go through Bitfinex's platform every month.
- As a high-frequency, financial trading platform, Bitfinex has two key priorities: speed and security. They wanted evenly distribute traffic across their front-end servers to avoid overload and ensure users were enjoying the fastest speeds possible.

SOLUTION

Bitfinex uses Cloudflare Load Balancing to split up traffic among their front-end servers — increasing network capacity and ensuring that servers are healthy. They also leverage Cloudflare's security suite — WAF and DDoS protection to block malicious requests from their servers.

VALUE

- Realized major savings in overhead with no more hardware to maintain
- Attained a user experience that's vastly easier to navigate — managing DNS, performance, and security needs into a single unified interface.
- Extensive API support for automation tasks and the Cloudflare Workers to build out custom functionality.

BITFINEX

"We considered rolling out our own solution, but at the end of the day Cloudflare's solution was more attractive: an existing platform that worked and allowed us to focus on developing our own offerings instead of reinventing the wheel."
— Adam Chamley
Developer

cloudflare.com/case-studies/bitfinex/

Say bye to the box

Ditch your legacy appliances for agile, scalable as-a-service application security

The problem with security appliances

Hardware security appliances are ill-matched to meet sophisticated, modern application attacks. Appliances are expensive to maintain and manage, require downtime, and unequipped to deal with traffic spikes stemming from attacks or high demand. Organizations must purchase new hardware every 3-7 years to keep pace with throughput needs as technology advances and enterprises scale. And when hardware undergoes upgrades or maintenance, security services will need to go offline, resulting in protection gaps. Appliances must also be right-sized to handle expected peak demand – leaving them either underutilized or unable to handle traffic over the expected levels, leaving applications defenseless.



Switching to cloud-based security not only helps organizations streamline their infrastructure and operations, but can lead to significant cost savings by eliminating hardware refreshes, reducing vendor sprawl, and cutting down on data center overhead.

The Cloudflare difference

Cloudflare's global network of edge servers reduces latency and improve website performance and security. Cloudflare offers a range of security features to help protect against a variety of web-based attacks, including DDoS protection, a web application firewall (WAF), and bot protection. Our cloud-native architecture means we are well-equipped to keep up with emerging threats – for example, as soon as our team of engineers release a new WAF rule for our managed rules, Cloudflare users will get those protections in production in 10-15 seconds. Cloudflare is a one-stop shop for consolidated security and performance: our single pane of glass solution for performance and security will help security teams identify and respond quickly to incidents.



Scalable and easy to use

Cloudflare lets organizations consume resources on an as-needed basis, and can absorb large DDoS attacks without impacting performance.

Cloudflare enables faster, automatic threat investigations and incident responses, while minimizing manual configuration and management.



Fast protections for emerging attacks

Backed by threat intelligence from a vast global network, Cloudflare's cloud-native security stack helps organizations meet these attacks head-on, without needing to wait for new security patches or appliance updates.



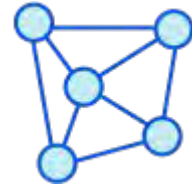
Cost effective

Cloudflare reduces valuable engineering hours spent on configuration and management so you can focus on your highest-priority initiatives.

We enable efficient growth so you only pay for the resources you need when you need them instead of paying hardware costs upfront.

Why is scalability so important to security?

Cloudflare allows users to draw on resources as needed to respond to traffic spikes during peak times, such as during a DDoS attack or a launch of a high-demand product. We also have unmetered DDoS and Rate Limiting solutions so that you don't have to worry about being hit with surge prices or struggle to allocate resources to defend your applications.



Our network can absorb even the largest DDoS attacks so your business can stay online.

See the comparison: Security appliance vendors vs Cloudflare

	Legacy security appliances	Cloudflare application security
Hardware costs	Hardware costs, including refreshes and data center overhead costs.	No hardware costs.
Engineering hours	Engineering costs can be high with many hours spent on complex scripting and maintenance overhead, including hardware and software lifecycle management.	Easy-to-use product means less engineering hours spent managing one vendor, which can free engineers up for higher-impact projects.
Security	Application security from appliance vendors: <ul style="list-style-type: none"> • Can be robust and customizable, but not very agile • Downtime for maintenance means applications are left unprotected • Unable to absorb or respond to the largest DDoS attacks on the Internet or handle peak traffic demands 	Security benefits of Cloudflare compared to appliance vendors: <ul style="list-style-type: none"> • Reduction of over 50% to the mean time to detect attacks • Our scale and global network allow us to quickly react to threats and detect 30%-40% more intrusion attempts • We typically reduce the mean time to remediate of such attacks by over 90%
Accounting impacts	Appliances are capital expenses: <ul style="list-style-type: none"> • Require upfront acquisition costs and then can be depreciated over years. • Enterprises need to acquire hardware to service peak requirements, but they will be under utilized during all other times. 	Operational expenses eliminate capital expenditures and depreciation: <ul style="list-style-type: none"> • Cloudflare's accounting benefits are more immediate • Cloudflare's operational expenditure model means customers can easily scale their environment to meet their specific needs without the upfront costs
Implementation time	<ul style="list-style-type: none"> • Hardware lead times (lengthened by supply chain issues) • Lengthy setup process • Often must script central management so configurations can be deployed consistently across all devices 	<ul style="list-style-type: none"> • Easy to centrally manage your security across all of your domains. • Cloudflare provides at least a 10X faster time to value compared to appliance vendors, even once the hardware is delivered and in place

Cloudflare Application Security Bundles



Security Bundles

What's included in App Security Bundles?

	Core (= WAF + Rate Limiting)	Advanced
Managed Rules	<ul style="list-style-type: none"> • Security Analytics • OWASP ruleset • Cloudflare Managed ruleset • Exposed Credentials Check ruleset • WAF Attack Score 	<ul style="list-style-type: none"> • Sensitive Data Detection
Custom Rules	<ul style="list-style-type: none"> • 1000 Custom Rules • 100 Basic Rate Limiting (IP-based) • Log and regex support 	<ul style="list-style-type: none"> • Account-level configuration • Advanced Rate Limiting* • Payload Inspection • Exposed Credentials Check custom rule
Threat Intel	<ul style="list-style-type: none"> • Managed IP List: Open Proxies 	<ul style="list-style-type: none"> • Managed IP lists: VPNs, Anonymizers, Malware, Botnets

Add-ons

Bot Management

- Bot Score
- Advanced detection engines

API Security/Shield

- Schema validation
- API Discovery
- API Abuse Detection (volumetric)
- API Sequential Abuse Detection
- Others

Page Shield

- Script monitor
- CSP and positive blocking

Content Scanning

- File upload Malware detection

* Advanced Rate Limiting can be bought a-la-carte on top of Core

Product overview

Web Application Firewall

Security Analytics

WHAT

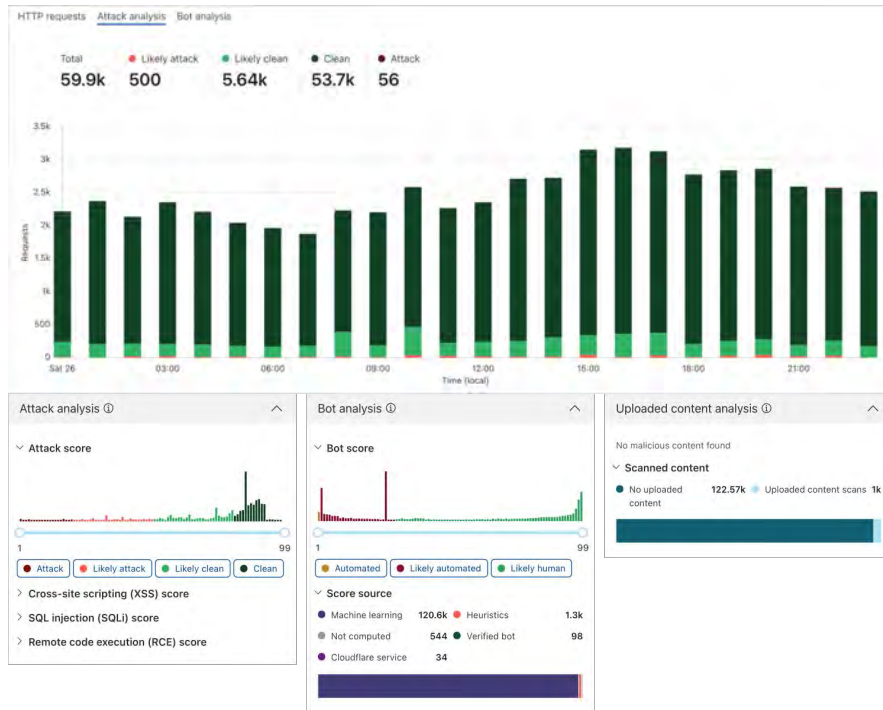
Cloudflare detections running on all customer traffic all the time bringing all products together.

WHY

Immediate ROI, increased visibility, much easier onboarding.

PLAN

Available to all ENT customers



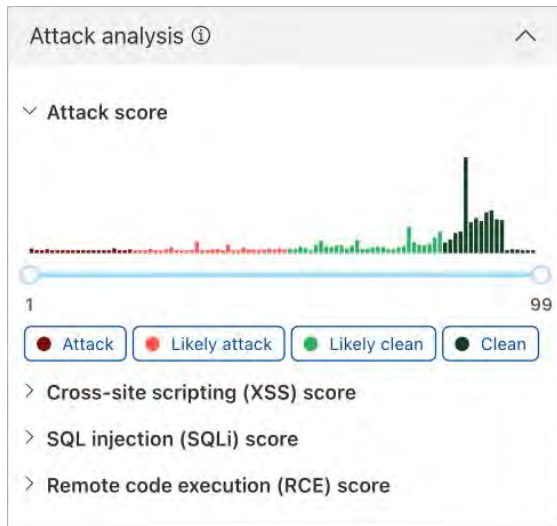
Web Application Firewall

Attack Score

WHAT Additional layer of protection against zero day vulnerabilities. ML model against WAF bypasses.

WHY Increased protection against attacks, we identify new exploits before they are made public

PLAN Available to all ENT customers



Exposed Credentials Check

WHAT

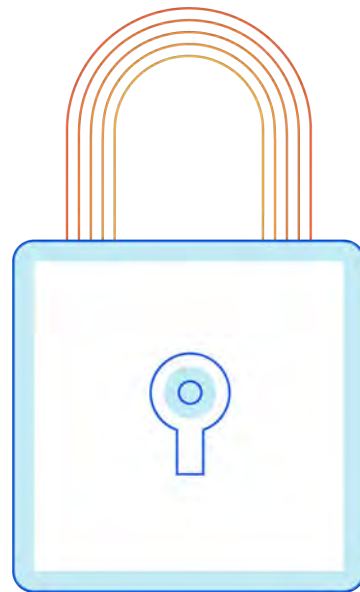
Customers are warned when an end-user logs into their application using a leaked credential; also useful for detecting and blocking credential stuffing attacks

WHY

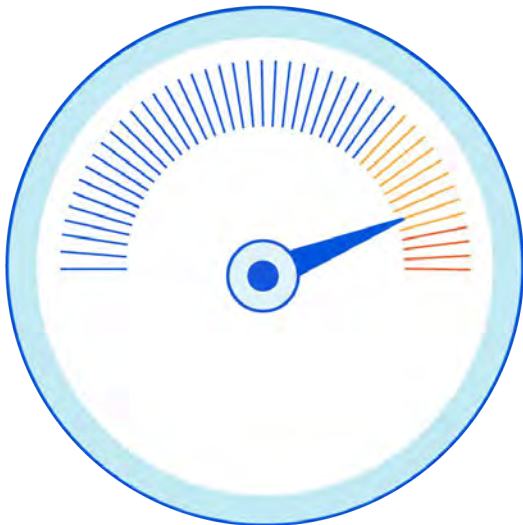
When breaches happen, hackers often use leaked credentials to try to take over accounts using compromised user accounts

PLAN

Managed Ruleset included with ENT plan. Custom rule requires Advanced.



Advanced Rate Limiting



WHAT

Specifically designed for APIs

- Rate Limit based on API Key, device/user ID, headers, JSON field, etc.
- Access request body to write rules for specific GraphQL / JSON fields
- Write rules with granular filters - e.g. different thresholds per Country, Bot Score, etc.

WHY

Move away from IP-based rate limiting

PLAN

Advanced or as add-on to Core

Account-level configuration



WHAT Account Level WAF configuration allowing for deployment of WAF rulesets on any subset of account traffic

WHY Easier-to-maintain and uniform configuration of thousands of applications

WHEN Available as part of Advanced

Payload inspection

WHAT

Customer can write Custom or Rate Limiting Rules accessing the body (or payload) of an HTTP request.

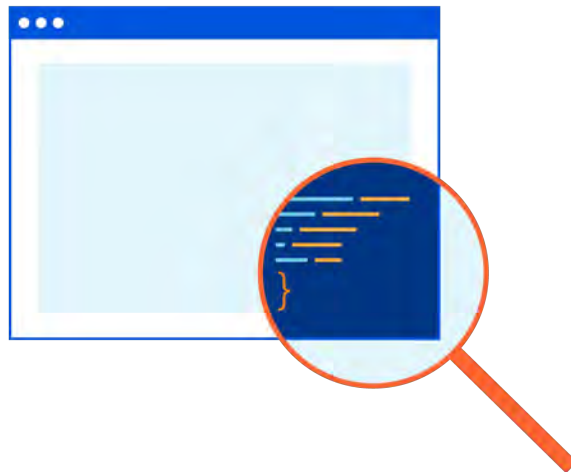
WHY

Example use cases include

- Block requests with unwanted keywords/fields
- Rate Limit based on the value of a JSON field (e.g. useful for GraphQL traffic)

PLAN

Included with Advanced



Web Application Firewall

Sensitive Data Detection

WHAT

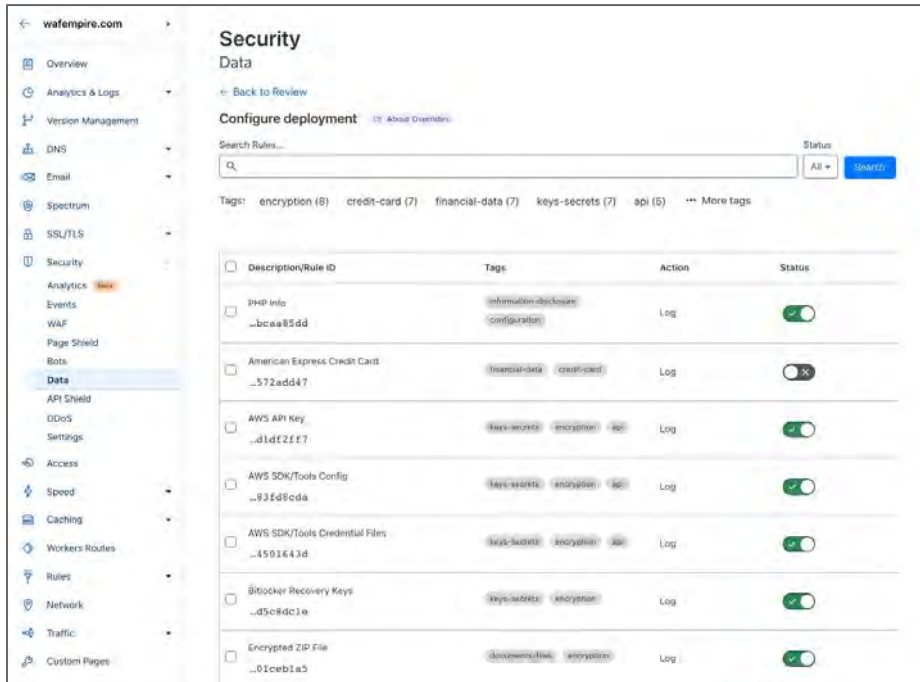
Runs on the response body and identifies when sensitive data or Personal Identifiable Information are being returned and logs it.

WHY

Identify successful data exfiltration attacks or accidental data leaks. Identify misconfigured or buggy APIs as a common source of exposed data

PLAN

Advanced



Security Data

← Back to Review

Configure deployment [About Overrides](#)

Search Rules... Status: All

Tags: encryption (8) credit-card (7) financial-data (7) keys-secrets (7) api (5) [More tags](#)

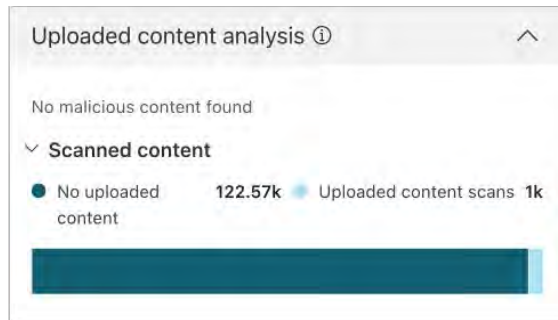
Description/Rule ID	Tags	Action	Status
<input type="checkbox"/> PHP Info ..bcaa85dd	information-disclosure configuration	Log	<input checked="" type="checkbox"/>
<input type="checkbox"/> American Express Credit Card ..572add47	financial-data credit-card	Log	<input type="checkbox"/>
<input type="checkbox"/> AWS API Key ..d1df2f17	keys-secrets encryption api	Log	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS SDK/Tools Config ..93fd8cda	keys-secrets encryption api	Log	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS SDK/Tools Credential Files ..4501643d	keys-secrets encryption api	Log	<input checked="" type="checkbox"/>
<input type="checkbox"/> Bitlocker Recovery Keys ..d5e8dc3e	keys-secrets encryption	Log	<input checked="" type="checkbox"/>
<input type="checkbox"/> Encrypted ZIP File ..01ceb1a5	documents/files encryption	Log	<input checked="" type="checkbox"/>

Content Scanning

WHAT Runs inline to HTTP requests and automatically detects when a file is uploaded. For any content object found, will run a scanning engine

WHY Protect applications from malware being uploaded

PLAN Available as add-on for ENT customers



Cloudflare Success Offerings

At Cloudflare, your success and trust matter to us. We are dedicated to being your advocates, product experts, and strategic advisors in helping you achieve your business and technical objectives.

Why should organizations choose Cloudflare Success Offerings?

Built for everyone

As your business grows, your Internet applications, network infrastructure, and teams become increasingly complex. We are committed to partnering with you and providing the right level of network infrastructure expertise at every stage of growth — whether you are just starting out, fully mature, or somewhere in between.

Highly trained, always online global support

Our 24/7/365 award-winning global support team delivers technical assistance around the clock to ensure your mission-critical priorities are also ours. We have a global team of best-in-class support engineers so you can focus on building your business without costly downtime or time-consuming technical issues.

Simple and predictable pricing

Our simple and predictable pricing for each offering makes it easy for you to create your budget and reduce the total cost of ownership.

Success Offerings: Standard & Premium

The **Standard Success Offering** helps you get started quickly with guided customer success-led onboarding, customer success guidance, and continued online support and training. You get access to 24/7/365 email, chat, and emergency phone support, on-demand technical resource guides, best practice product implementation multimedia, and advanced reporting capabilities, no matter your business size.

Included with Cloudflare Enterprise subscriptions.

The **Premium Success Offering** includes everything in the Standard Success Offering plus a dedicated success team assigned to your account that provides highly customized tuning and strategic assistance at every step along the way. The Premium Success Offering is ideal for large and rapidly growing enterprises that require one-on-one guidance, have complex technical environments, and need enhanced support service at rapid response times.

With this offering, you gain exclusive access to Cloudflare's early adopter program, a designated incident response team, proactive monitoring and alerting (in beta), and many more highly customized services.

Available for purchase at +20% on top of your Cloudflare Enterprise Product subscription.



Success Offering Features

Premium offering available for annual contract value between \$100,000 - \$749,000.

	Standard	Premium
Onboarding		
Access To Enterprise Customer Portal	✓	✓
Customer Success Led Onboarding Assistance	✓	✓
Designated Customer Success Manager	✓	✓
Guided Onboarding Experience	×	✓
Expert Tuning Workshop	×	✓
Optimized Experience		
Annual Health Check	✓	✓
Monthly Operational Review [email]	✓	✓
Periodic Executive Business Review	×	✓
Access To Tuning With Senior Technical Experts	×	✓
Review Of Product Releases	×	✓
Office Hours With Product Management Team	×	✓
Early Adopter Program Access	×	✓
Technical Support		
Access To Support Community	✓	✓
24/7 Email And Chat Support	✓	✓
Emergency Phone Support Hotline	✓	✓
Under Attack Support Engineer For Magic Transit	×	✓
Prioritized Case Handling	×	✓
Availability SLA Credit	10x Credit	25x Credit
Technical Support Response SLA		
P1 - Urgent	<2 Hr	<1 Hr
P2 - High	<4 Hr	<2 Hr
P3 - Normal	<48 Hr	<24 Hr
P4 - Low	<48 Hr	<24 Hr
Training/Education		
Access To Online Documentation	✓	✓
Access To Online Training Workshops	✓	✓
Use Case Optimization Workshops	×	✓
Customized Training Workshops	×	✓
Reporting		
Cache Analytics Insights	✓	✓
Health Check Analytics Insights	✓	✓
Customized Usage And Value Reporting	×	✓

Getting started: Contact your Cloudflare Account Executive today to get started.

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

Section 1. Purchase Order.

A. Composition and Priority.

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

B. Initial Term.

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

Section 2. Performance.

A. Performance Standards.

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

B. Performance Deficiency.

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

Section 3. Payment and Fees.

A. Payment Invoicing.

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

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

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

B. Payment Timeframe.

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

C. MyFloridaMarketPlace Fees.

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

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

D. Payment Audit.

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

E. Annual Appropriation and Travel.

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

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

Section 4. Liability.

A. Indemnity.

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

B. Payment for Claims.

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

C. Liability Insurance.

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

D. Workers' Compensation.

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

E. Performance Bond.

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

Section 5. Compliance with Laws.

A. Conduct of Business.

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

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

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

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

B. Lobbying.

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

C. Gratuities.

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

D. Cooperation with Inspector General.

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

E. Public Records.

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

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

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

F. Communications and Confidentiality.

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

G. Intellectual Property.

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

H. Convicted and Discriminatory Vendor Lists.

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

Section 6. Termination.

A. Termination for Convenience.

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

B. Termination for Cause.

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

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

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

Section 7. Subcontractors and Assignments.

A. Subcontractors.

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

B. Assignment.

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

Section 8. RESPECT and PRIDE.

A. RESPECT.

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

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

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

B. PRIDE.

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

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

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

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

Section 9. Miscellaneous.

A. Independent Contractor.

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

B. Governing Law and Venue.

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

C. Waiver.

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

D. Modification and Severability.

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

E. Time is of the Essence.

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

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

F. Background Check.

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

G. E-Verify.

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

H. Commodities Logistics.

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

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

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK



4050 Esplanade Way
Tallahassee, FL 32399-0950

Ron DeSantis, Governor
Pedro Allende, Secretary

**CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT
BETWEEN
FLORIDA DEPARTMENT OF MANAGEMENT SERVICES
AND
Presidio Networked Solutions, LLC**

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

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

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

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

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

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

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

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

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

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

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

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

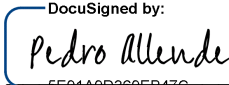
- 12. Governing Law and Venue.** The laws of the State of Florida govern the Agreement. The Parties submit to the jurisdiction of the courts of the State exclusively for any legal action related to the Agreement which arises during or after the Agreement term. Further, Recipient hereby waives all privileges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


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

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

**FLORIDA DEPARTMENT
OF MANAGEMENT SERVICES**

Presidio Networked Solutions, LLC

DocuSigned by:

By: _____
5E91A9D369EB47C...
Name: Pedro Allende
Title: Secretary
Date: 6/14/2023 | 4:59 PM EDT

By:  _____
Name: Jay Staples
Title: Assistant General Counsel
Date: 5/23/2023