



**State Term Contract
No. 43230000-24-STC
For
Digital Security Solutions**

This State Term Contract No. 43230000-24-STC("Term Contract") is between the Department of Management Services ("Department"), an agency of the State of Florida, located at 4050 Esplanade Way, Tallahassee, Florida 32399; and Nethive LLC ("Contractor") with its principal place of business located at 172 Heimatsweg, Chapin, SC 29036; collectively referred to herein as the "Parties."

WHEREAS, the Department issued a competitive solicitation for Digital Security Solutions; and

WHEREAS, the Contractor was awarded as a result of such competitive solicitation to offer the following proposed Solution(s):

NOW THEREFORE, in consideration of the mutual promises contained herein, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

I. Term and Effective Date.

The initial term of the Term Contract shall be for 2 years. The Term Contract will become effective on March 1, 2025 , or on the date signed by all Parties, whichever is later. The Term Contract shall expire on February 28, 2027 unless terminated earlier or renewed in accordance with Exhibit C, Enterprise Standard Terms and Conditions.

II. Order of Precedence.

This contract document and the attached exhibits constitute the Term Contract and the entire understanding of the Parties. All Exhibits listed below are incorporated into this Term Contract by reference herein. In the event of a conflict, the Term Contract document and Exhibits shall have priority in the following order:

- a) This contract document
- b) Exhibit A, Scope of Work
- c) Exhibit B, Price Sheet
- d) Exhibit C, Enterprise Standard Terms and Conditions
- e) Exhibit D, Technical Response(s) to the competitive solicitation
- f) Exhibit E, PUR 7801
- g) Exhibit F, Solution Service Level Agreements
- h) Exhibit G, Solution Additional Terms and Conditions

State Term Contract No. **No. 43230000-24-STC**
For
Digital Security Solutions

III. Purchases off this Term Contract.

Upon execution of this Term Contract, Customers, as defined in Exhibit D, Enterprise Standard Terms and Conditions, may purchase products and services under this Term Contract. Any entity making a purchase off of this Term Contract acknowledges and agrees to be bound by the terms and conditions of this Term Contract. The Contractor shall adhere to the terms included in any contract or purchase orders issued pursuant to this Term Contract.

IV. Primary Contacts.

Department's Contract Manager:

Christopher McMullen
Division of State Purchasing
Florida Department of Management Services
4050 Esplanade Way, Suite 360
Tallahassee, Florida 32399-0950
Telephone: (850) 922-9867
Email: Christopher.mcmullen@dms.fl.gov

Contractor's Contract Manager:

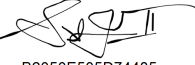
Beth Warren
Nethive LLC
172 Heimatsweg
Chapin, SC 29036
Telephone: (888) 638-9824
Email: sales@netwatch.ai

Either party may notify the other by email of a change to a designated Contract Manager providing the contact information for the newly designated contact, and such notice is sufficient to effectuate this change without requiring a written amendment to the Term Contract.

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

State Term Contract No. **No. 43230000-24-STC**
For
Digital Security Solutions

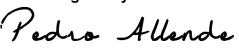
Nethive LLC

Signed by:

B2050E505D74485...

Stephen Franklin

3/18/2025 | 1:12 PM PDT

Date:

**STATE OF FLORIDA,
DEPARTMENT OF
MANAGEMENT SERVICES**
DocuSigned by:

C94713929499485...

Pedro Allende, Secretary

3/20/2025 | 12:29 PM EDT

Date:

Exhibit A

Scope of Work

1. Purpose

To provide Customers with statewide Digital Security Solutions, pursuant to the terms set forth in this Scope of Work. Digital Security Solutions must be provided in accordance with Chapter 282, Florida Statutes (F.S.), Rule Title 60GG, Florida Administrative Code (F.A.C.), and cybersecurity best practices. Digital Security Solutions 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.

2. Definitions

Definitions contained in section 287.012, F.S.; Rule 60A-1.001, F.A.C.; Attachment D, Enterprise Standard Terms and Conditions; and the PUR 1000, General Contract Conditions, are incorporated by reference. In the event of a conflict, the definitions listed in this section supersede the incorporated definitions for the purposes of this Scope of Work. All definitions apply in both their singular and plural sense.

Add-On Services – Non-core or additional services available for purchase to enhance or support a Solution.

Business Day – Monday through Friday, inclusive, except for those holidays specified in section 110.117, F.S., from 8:00 a.m. to 5:00 p.m. at the Customer's location.

Commodity Code – The State's numeric code for classifying commodities and contractual services which meet specific requirements, specifications, terms, and conditions herein. Florida has adopted the United Nations Standard Products and Services Code (UNSPSC) for classifying commodities and services.

Confidential Information – Information that is trade secret or otherwise confidential or exempt from disclosure under Florida or federal law.

Contract Manager – The representative designated by the Department who will oversee all aspects of the Contract, monitor performance expectations, and serve as the primary point of contact for the Contractor.

Criminal Justice Information Services (CJIS) – Services providing access to national or local criminal justice information.

Digital Security Solutions(s) – The products, services, or software that meet the needs of a Service Category. May be used interchangeably with Solution.

Identity and Access Management Systems (IAM) – A Framework that provides/controls user access to critical information within their organization.

International Organization for Standardization (ISO) – An independent, non-governmental, international standard development organization composed of representatives from the national standards organization of member countries.

Manufacturer – The producer or provider of Digital Security Solutions. May be used interchangeably with Brand Name.

Service Category(ies) – The categories of products and services under this Contract. The Service Categories are: Endpoint-Based Asset Discovery; Network-Based Asset Discovery; Endpoint Detection and Response; External-Facing Asset Discovery; Email Security; Content Delivery Network; Security Operations Platform (SOP); Identity and Access Management (IAM); Mobile Security and Threat Detection; Secure Access Service Edge (SASE); Governance, Risk, and Compliance (GRC); IT Service Management (ITSM); Vulnerability Assessment and Management; Cybersecurity Threat Intelligence (CTI), Data Security, and Enterprise Security Log Management, Analytics, and Response.

Value-Added Services - Value-added services include any additional services the Contractor offers, for no additional cost to the Customer, as part of the Term Contract, and which clearly exceed the minimum requirements and are within the scope of this Term Contract. An example of value-added services would be, “The Contractor will provide a year of 24/7 support services, at no cost to the Customer.” Any value-added service proposed by the Contractor, if accepted by the Customer, shall become a requirement and be a part of the minimum service specifications contained in any resulting Purchase Order.

3. Scope of Work

3.1 Digital Security Solutions Requirements:

All Solutions shall adhere to the following minimum specifications:

3.1.1 Compliance

Solution shall comply with relevant industry standards and regulations applicable to the State of Florida and the relevant state agency (e.g., CJIS, HIPAA, SOX, PCI-DSS, NIST CSF).

3.1.2 Scalability

Solution shall scale to accommodate current and future growth of the Customer, handling both increased workloads and expansion across additional devices, users, or systems.

3.1.3 Reliability

Solution shall provide high availability and reliability, with minimal downtime and robust disaster recovery capabilities to ensure business continuity.

3.1.4 Interoperability

Solution shall have the ability to, in response to a Customer Request for Quote, provide seamless integration with Customer systems, applications, and infrastructures detailed in the Request for Quote, ensuring that the Solution can coexist within the Customer IT ecosystems without requiring major overhauls.

3.1.5 User-Friendly Interface

Solution shall provide an intuitive and easy-to-use interface for both IT staff and end-users, ensuring that tasks can be performed efficiently regardless of the technical proficiency of the user.

3.1.6 Data Protection

Solution shall ensure data is encrypted both at rest and in transit using industry-standard encryption algorithms.

3.1.7 Access Controls

Solution shall include Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) for managing user access. Comprehensive logging and auditing capabilities to track data access, configuration changes, and security events.

3.1.8 Confidentiality Agreements

Solution shall have the ability to implement and enforce confidentiality agreements between Customers and the Contractor upon request of the Customer.

3.1.9 API and SDK Availability

Solution shall provide availability of APIs and SDKs for custom integrations and extending functionality where needed.

3.1.10 Support for Cloud and On-Premise Environments

Solution shall support hybrid environments, including cloud-based, on-premises, and multi-cloud deployments where applicable.

3.1.11 Log Forwarding

Solution shall, where feasible, be able to integrate logs with external log aggregation systems such as SIEMs, ensuring that critical data is available for analysis and audit purposes.

3.1.12 Staff Training

Solution shall include training sessions on best practices and implementation. Ongoing training resources shall be made available as part of the Solution to ensure staff are knowledgeable about the Solution.

3.1.13 Ongoing Support

Solution shall provide availability of ongoing support and consultation services, including SLAs for issue resolution and dedicated account managers or customer success teams.

3.1.14 Documentation and Resources

Solution shall provide access to comprehensive documentation, user guides, and online resources for continuous learning and improvement. Regular webinars, user community forums, and/or knowledge-sharing platforms to keep users informed of updates or best practices.

The Technical Response Attachments L1-L16 define the requirements for the Service Categories. A Technical Response, submitted for an awarded Solution named therein, along with any provided Solution Service Level Agreements, shall form part of a Vendor's resulting Term Contract. The Service Categories, as detailed below and in the Technical Response

Attachments, define the expected functions and objectives of each Service Category, giving Vendors a clear understanding of what is needed to support the State of Florida's digital security and operational requirements.

Each Service Category includes a detailed description of the Solution's purpose that a Solution must address, followed by a section which includes "Solutions should provide", which lists the technical capabilities and features that are generally expected for a Solution. Vendors are encouraged to propose Solutions that meet these capabilities; however, it is not required for a Solution to fulfill every part of the listed capabilities. Instead, the intent is to provide a comprehensive guideline for Vendors to design and tailor their Solution in alignment with the State's needs, while allowing flexibility based on the strengths and specific functionalities of its offering.

3.2 Service Category 1: Endpoint-Based Asset Discovery:

An Endpoint-Based Asset Discovery Solution must continuously scan, detect, and inventory all endpoint devices, including, but not limited to laptops, desktops, servers, and any other connected devices across the enterprise. The Solution must utilize lightweight agents that are deployed via endpoints, consuming minimal CPU and memory resources to avoid degrading performance or user experience.

The Service Category 1: Endpoint-Based Asset Discovery should provide:

3.2.1 Real-Time Asset Discovery

Solution should run continuously, detecting new devices as they connect to the network. This should include remote devices.

3.2.2 Detailed Hardware and Software Inventories

Solution should include inventory of processor types, memory, storage, installed software, patch levels, operating system versions, and device configurations.

3.2.3 Customizable Asset Classifications

Solution should allow administrators to tag devices by type, location, or business unit for easier management.

3.2.4 Agent Health Monitoring

Solution should ensure that agents are functioning correctly and can be managed or repaired from a central console, if necessary. The Solution should provide alerts if an agent becomes inactive or fails to report.

3.2.5 Centralized Management Console

Solution should provide a centralized management console that displays an up-to-date view of all discovered endpoints, including non-standard devices such as personal mobile devices or tablets.

3.2.6 Compliance Enforcement

Solution should provide alerts to where endpoints that fail to meet security requirements (e.g., outdated patches or unauthorized software) can be flagged for remediation.

3.2.7. Integration of CTI Data Feeds

Solution should provide real-time insights into endpoint vulnerabilities, ensuring that newly discovered devices are checked against the latest IoCs (Indicators of Compromise) and CVEs (Common Vulnerabilities and Exposures) behaviors targeting specific operating systems or device types.

3.2.8 Patching and Deployment Capability

Solutions should provide endpoint patch and deploy services which allows managing patch and deployment of operating system and application updates on systems utilizing the agent.

3.2.9 Metrics

Solution should provide the ability to roll-up patch and deployment level metrics across the domain.

3.3 **Service Category 2: Network-Based Asset Discovery:**

A Network-Based Asset Discovery Solution identifies devices and systems communicating within the network infrastructure without the need for software agents to be deployed to most endpoints or servers. By analyzing network traffic, the Solution should detect all connected assets, including those that do not run traditional operating systems, such as Internet of Things (IoT) devices, switches, routers, and printers.

The Service Category 2: Network-Based Asset Discovery should provide:

3.3.1 Agentless Discovery

Solution should be capable of using passive network scanning techniques that observe network traffic and communications, including deep packet inspection (DPI) and flow-based analysis.

3.3.2 Continuous Network Monitoring

Solution should automatically detect new devices as they are added to the network, whether they are traditional endpoints, virtual machines, or IoT devices.

3.3.3 Granular Device Identification

Solution should collect metadata such as MAC address, IP address, operating system, software versions, device make and model and open ports.

3.3.4 Network Topology Visualization

Solution should map discovered devices and displays how they connect and communicate within the network. The visualization should dynamically update as devices are added, removed, or reconfigured.

3.3.5 Customizable Device Grouping and Tagging

Solution should allow administrators to categorize assets based on network segment, physical location, or function (e.g., servers, IoT, printers).

3.3.6 Vulnerable Detection

Solution should identify outdated software versions, unpatched firmware, or insecure configurations that could expose the network to threats.

3.3.7 Integration of CTI Data Feeds

Solution should provide real-time insights into suspicious network activity, such as communication with known malicious IP addresses or domains. Solution should flag devices that may be compromised or communicating with threat actors.

3.4 **Service Category 3: Endpoint Detection and Response:**

An Endpoint Detection and Response Solution is designed to provide continuous and comprehensive monitoring of endpoint activities to detect, investigate, and respond to threats in real-time. The Solution collects and analyzes detailed telemetry data, such as file access patterns, process execution, network connections, and registry changes, to identify malicious behavior that traditional antivirus software might miss.

The Service Category 3: Endpoint Detection and Response should provide:

3.4.1. Real-Time Monitoring and Logging

Solution should provide real-time monitoring and logging of all endpoint activities, including, but not limited to, file changes, process creation and termination, registry edits, network connections, and USB device insertion.

3.4.2. Behavioral Analytics

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

3.4.3. Forensic Capabilities

Solution should allow security analysts to investigate historical endpoint activities, enabling root cause analysis and providing a detailed timeline of events leading up to a security incident.

3.4.3. Automated Response Mechanisms

Solution should take predefined actions when threats are detected, such as isolating the affected device from the network, terminating malicious processes, or blocking IP addresses.

3.4.4 Threat Hunting Tools

Solution should allow analysts to query across the entire organization's endpoints, searching for specific indications or compromise (IoCs) or patterns that may indicate the presence of advanced threats.

3.4.5 Support for Remote Endpoints

Solution should ensure that devices outside of the network, such as remote or mobile works, are protected and monitored regardless of location.

3.4.6 Remediation Playbooks

Solution should provide detailed guidance for resolving detected incidents, including step-by-step instructions for isolating infected devices, rolling back malicious changes, and restoring systems to a known good state.

3.4.7 Integration of CTI Data Feeds

Solution should provide real-time updates on emerging malware strains, threat actor campaigns, and new attack vectors targeting endpoints. The EDR Solution can use CTI feeds to compare endpoint behavior when known IoCs, enhancing detection and automated response capabilities.

3.4.8. Forensic Capabilities

Solution should allow security analysts to investigate historical endpoint activities, enabling root cause analysis and providing a detailed timeline of events leading up to a security incident.

3.5 **Service Category 4: External-Facing Asset Discovery:**

External-Facing Asset Discovery Solutions must help organizations identify and assess the security of their publicly accessible digital assets, such as web servers, cloud services, applications, and other internet-facing systems. The Solution must continuously scan the organization's external IP ranges and domains to identify assets that are exposed to the internet and assess their vulnerabilities.

The Service Category 4: External-Facing Asset Discovery should provide:

3.5.1 Continuous Scanning

Solution should provide continuous scanning of public IP addresses and domains associated with the organization, identifying all internet-facing services, applications, and network devices.

3.5.2 Service Detection and Banner Grabbing

Solution should collect information such as service versions, SSL/TLS certificate details, and software configurations for each exposed asset.

3.5.3 Identification of Outdated Software

Solution should identify outdated software or insecure configurations, such as weak SSL certificates, open ports, misconfigured DNS settings, or vulnerable software versions that could be exploited by attackers.

3.5.4 Integration with Vulnerability Databases

Solution should integrate with vulnerability databases such as CVE, CWE, and the National Vulnerability Database to provide immediate context around known vulnerabilities affecting identified services or software.

3.5.5 Risk Scoring

Solution should accommodate risk scoring of external assets, prioritizing those that are most vulnerable to exploitation or are most critical to business operations.

3.5.6 Customizable Alerting

Solution should notify security teams when a new external asset is detected, a known vulnerability is identified, or a change in configuration occurs (e.g., a certificate has expired).

3.5.7 Integration of CTI Data Feeds

Solution should correlate external-facing assets with current threat actor campaigns or vulnerabilities that are actively being exploited. This ensures that publicly exposed services are continuously monitored against known threats in real-time.

3.6 **Service Category 5: Email Security:**

Email Security Solutions must protect against email-based threats such as phishing, malware, ransomware, and email compromises. The Solution should analyze both inbound and outbound email communications in real-time, using advanced detection techniques to filter malicious content without disrupting legitimate business correspondence.

The Service Category 5: Email Security should provide:

3.6.1 Content Filtering

The Solution should break down files to their discrete components in real-time and reconstruct a clean version of the email, removing anything that doesn't conform with the file type specifications, a nationally recognized standard, or company policy.

3.6.2 Phishing Detection

Solution should analyze the email's context, structure, and metadata (e.g., header

information) to detect phishing attempts, which may include spear-phishing and targeted attacks.

3.6.3 Sandboxing Technology

Solution should have the capability to safely execute email attachments and embedded links in an isolated environment to determine if they are malicious before delivery to the recipient.

3.6.4 Advanced Anti-Spoofing Protections

Solution should include enforcement of Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocols to prevent sender impersonation.

3.6.5 Email Encryption

Solution should include encryption for sensitive communications, ensuring enforcement that messages are encrypted both in transit and at rest.

3.6.6 End-User Awareness Features

Solution should include automatic banners or warnings added to suspicious emails, helping users recognize potential threats.

3.6.7 Quarantine and Remediation Tools

Solution should provide quarantine and remediation tools for administrators, allowing them to review flagged messages, release legitimate emails mistakenly identified as threats, and block harmful content.

3.7 Service Category 6: Content Delivery Network:

A Content Delivery Network (CDN) optimizes the delivery of web content by distributing it across a network of edge servers located globally. This reduces latency, improves page load times, and enhances the user experience, especially for content-heavy websites or applications. The Solution must ensure secure and efficient content delivery, while providing protection against common web-based attacks through mitigation of attacks such as distributed denial of service or web application exploits.

The Service Category 6: Content Delivery Network should provide:

3.7.1 Distributed Edge Server Architecture

Solution should allow content to be cached and served from the server closest to the end-user to reduce latency and improve performance.

3.7.2 Support for Dynamic Content Acceleration

Solution should optimize the delivery of personalized or frequently updated content through intelligent routing and caching mechanisms.

3.7.3 Content Caching Controls

Solution should allow administrators to define TTL (time-to-live) values, cache purging rules, and caching policies that align with the organization's needs.

3.7.4 Integrated DDoS Mitigation

Solution should protect web applications from volumetric attacks by filtering malicious traffic before it reaches the origin server.

3.7.5 Integrated Web Application Firewall

Solution should protect web applications from exploits.

3.7.6 Real-Time Traffic Analytics

Solution should provide insights into website traffic, user behavior, cache hit/miss ratios, and security incidents such as DDoS attempts or SSL handshake failures

3.7.7 Customizable Caching Rules

Solution should allow selective caching of specific content types (e.g., static images, JavaScript files, or video files) and exclusion of sensitive or dynamic data from the cache.

3.7.8 Integration of CTI Data Feeds

Solution should allow the CDN to identify and block traffic from known malicious IP addresses or domains, as well as protecting against emerging DDoS threats flagged by threat intelligence.

3.8 **Service Category 7: Security Operations Platform:**

The Security Operations Platform (SOP) must integrate multiple security tools and technologies into a single unified platform, providing comprehensive visibility into an organization's IT environment. The Solution should allow security teams to detect, investigate, and respond to threats in real-time, correlating data from across the infrastructure to provide a holistic view of security incidents.

The Service Category 7: Security Operations Platform should provide:

3.8.1 Log Event Aggregation and Correlation

Solution should log event aggregation and correlation from various security devices (firewalls, IDS/IPS, endpoint detection tools, network devices, and cloud services) to identify patterns and indicators of compromise.

3.8.2 Automated Incident Response Workflows

Solution should allow security operations teams to optionally automate common tasks such as blocking IP addresses, isolating infected devices, or generating alerts for further investigation.

3.8.3 Real-Time Threat Detection

Solution should be powered by machine learning models and behavioral analytics, capable of identifying zero-day attacks, insider threats, and anomalous activities that deviate from the organization's baseline.

3.8.4 Customizable Dashboards

Solution should have dashboards displaying real-time security metrics, providing visualizations of key performance indicators (KPIs) such as the number of incidents, time-to-respond, or threat severity.

3.8.5 Incident Management Capabilities

Solution should provide detailed incident tracking, ticketing integration, and root cause analysis, ensuring that all security events are fully documented and addressed.

3.8.6 Integration with Threat Intelligence Platforms (TIPs)

Solution should enrich security alerts with contextual information about current threat actors, malware campaigns, and indicators of compromise

3.8.7 Integration of CTI Data Feeds

Solution should Allow for real-time enrichment of alerts, correlating incidents with known global threat actor campaigns, IoCs, and TTPs (Tactics, Techniques, and Procedures), improving situational awareness and response times.

3.9 **Service Category 8: Identity and Access Management (IAM):**

IAM Solutions must provide centralized management for digital identities and control access to systems and data based on organizational policies. The Solution should manage the full lifecycle of user identities, from onboarding to de-provisioning, and enforce access control through role-based (RBAC) and attribute-based (ABAC) mechanisms.

The Service Category 8: Identity and Access Management (IAM) should provide:

3.9.1 Single Sign-On (SSO)

Solution should be compatible across on-premise and cloud based applications, reducing password fatigue and ensuring a seamless login experience for users.

3.9.2 Multi-Factor Authentication (MFA)

Solution should provide enforcement, supporting various authentication methods (e.g., Time-based one-time Password (TOTP), Short Message Service (SMS), biometrics) to add an extra layer of security.

3.9.3 Role-Based Access Control (RBAC) and Attribute-Based Control (ABAC)

Solution should include mechanisms, enabling fine-grained access permissions based on user roles or attributes such as location, department, or security clearance.

3.9.4 Federated Identity Management

Solution should allow cross-domain authentication using standard protocols like Security Assertion Markup Language (SAML), Open Authorization (OAuth), and OpenID Connect.

3.9.5 Privileged Access Management (PAM)

Solution should provide capabilities to control and monitor the use of administrative or high-privilege accounts, ensuring that elevated access is limited and auditable.

3.9.6 Self-service Functionality

Solution should allow users to manage their own passwords, request access to systems, and track the status of access requests through an approval workflow.

3.9.8 Integration of CTI Data Feeds

Solution should allow the IAM system to detect compromised credentials, suspicious login attempts, or help identify identity-related threat actor activities in real-time.

3.10 Service Category 9: Mobile Security and Threat Detection:

Mobile Security Solutions must protect mobile devices (smartphones, tablets, and laptops) from unauthorized access, data leakage, and malware while maintaining compliance with security policies. The Solution should work across iOS, Android, and other mobile operating systems, integrating with Mobile Device Management (MDM) platforms to enforce security policies and track compliance.

The Service Category 9: Mobile Security and Threat Detection should provide:

3.10.1 Mobile Threat Detection

Solution should include capabilities that monitor device behavior, app activity, and network connections for suspicious activities such as unauthorized data access, unapproved app installations, or malware downloads.

3.10.2 Mobile Application Management (MAM)

Solution should manage and secure the use of both enterprise and personal apps on mobile devices, including the ability to blacklist unsafe apps or restrict certain app permissions.

3.10.3 Device Encryption Enforcement

Solution should ensure that all data stored on the device is encrypted using industry-standard encryption algorithms (AES-256).

3.10.4 Remote Wipe and Lock Capabilities

Solution should enable administrators to remotely erase data from lost or stolen devices to prevent unauthorized access.

3.10.5 VPN Enforcement

Solution should ensure that all mobile data traffic is securely transmitted through encrypted channels, even when using public Wi-Fi networks.

3.10.6 Behavioral Analytics

Solution should identify anomalous activities on mobile devices, such as attempts to bypass security controls or connect to unauthorized networks.

3.10.7 Integration with MDM Solutions

Solution should enforce policies for password strength, screen lock timers, device encryption, and software updates.

3.10.8 Geo-Fencing Capabilities

Solution should allow administrators to restrict device functionality or access based on geographic location.

3.10.9 Integration of CTI Data Feeds

Solution should detect mobile-specific malware, phishing campaigns, or command-and-control traffic targeting mobile devices, providing real-time intelligence to block such threats.

3.11 Service Category 10: Secure Access Service Edge (SASE):

SASE Solutions combine networking and security services, delivering both through a cloud-based framework that supports remote users, branch offices, and cloud applications. The Solution integrates Software-Defined Wide Area Networking (SD-WAN) with advanced security features like Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS).

The Service Category 10: Secure Access Service Edge (SASE) should provide:

3.11.1 SD-WAN with Policy-Based Routing

Solution should enable dynamic, intelligent path selection to ensure optimal network performance for applications, even across distributed cloud environments.

3.11.2 Zero Trust Network Access (ZTNA) Principles

Solution should enforce least-privilege access to applications based on identity and context (e.g., user role, device health, location) rather than assuming trust based on network location.

3.11.3 Secure Web Gateway (SWG)

Solution should include features that protect users from web-based threats, such as malware, malicious URLs, and phishing attempts, by inspecting traffic at the cloud edge and enforcing acceptable use policies.

3.11.4 Firewall as a Service (FWaaS)

Solution should deliver consistent firewall policies across multiple locations and devices, centralizing management of security controls such as network segmentation, access control, and intrusion detection.

3.11.5 Real-Time Analytics and Reporting

Solution should provide insights into network performance, traffic patterns, security threats, and user behavior across distributed environments.

3.11.6 Integration of CTI Data Feeds

Solution should detect and block malicious network traffic or unauthorized access attempts based on real-time threat intelligence, correlating user activity and network behavior with known threat actors or compromised infrastructure.

3.11.7 Cloud Access Security Broker (CASB)

Solution should integrate to provide visibility and control over cloud applications and services, monitoring and securing data stored in third-party SaaS platforms.

3.12 Service Category 11: Governance, Risk, and Compliance (GRC):

GRC Solutions should provide a structured approach to managing governance frameworks, assessing enterprise risks, and ensuring compliance with industry regulations. The Solution must facilitate the development of policies, automate compliance checks, and enable risk management and assessment workflows that align with business objectives.

The Service Category 11: Governance, Risk, and Compliance (GRC): should provide:

3.12.1 Centralized Policy Management

Solution should allow the creation, distribution, and tracking of governance frameworks, compliance guidelines, and operational policies. The Solution should support version control and electronic signatures for policy acceptance.

3.12.2 Risk Assessment Tools

Solution should enable organizations to identify, assess, and prioritize risks across departments or business units based on likelihood and impact.

3.12.3 Risk Mitigation and Treatment Workflows

Solution should allow teams to define and track risk response plans, assign responsibilities, and monitor progress toward mitigation goals.

3.12.4 Audit Management Capabilities

Solution should support the planning, scheduling, and execution of internal and external audits. The platform should automatically generate audit reports, track findings, and ensure follow-up actions are completed.

3.12.5 Compliance Tracking

Solution should include industry-specific regulations (e.g., NIST CSF, GDPR, HIPAA, PCI-DSS), with automated controls and real-time monitoring to detect non-compliance or control failures.

3.12.6 Customizable Risk Dashboards

Solution should provide executives with an overview of key risks, compliance metrics, and the overall health of the governance program. Dashboards should display real-time data and support drill-down views for detailed analysis.

3.12.7 Third-Party Risk Management

Solution should facilitate the assessment of third-party vendor risks and perform due diligence on vendors' compliance and risk management practices.

3.13 Service Category 12: IT Service Management (ITSM):

ITSM Solutions are designed to streamline the delivery and management of IT services by providing a structured approach to incident management, problem resolution, change control, and service request fulfillment. The Solution should support automation, self-service capabilities, and detailed reporting on service levels.

The Service Category 12: IT Service Management (ITSM) should provide:

3.13.1 Automated Incident Management Workflows

Solution should detect, categorize, and prioritize IT incidents based on predefined rules. The system should support automatic escalation and notification of incidents to the appropriate teams.

3.13.2 Self-Service Portal

Solution should enable end-users to submit service requests, track the status of requests, and access knowledge base articles for self-help. The portal should integrate with automated fulfillment workflows, reducing the need for manual intervention.

3.13.3 Change Management Tools

Solution should include request and approval workflows, risk assessment for changes, and automated enforcement of change windows and rollback plans.

3.13.4 Configuration Management Database (CMDB)

Solution should track all configuration items (CIs) within the IT infrastructure, including hardware, software, networks, and cloud assets. The CMDB should map dependencies between CIs and provide insights into potential impact during incident resolution or change requests.

3.13.5 Service Level Management

Solution should define, monitor, and report on Service Level Agreements (SLAs). The system should automatically calculate performance metrics such as response time, resolution time, and service availability, and provide real-time dashboards.

3.13.6 Pre-Built Integrations

Solution should include monitoring tools, security platforms, and asset management systems to provide full visibility into the health and performance of IT services.

3.13.7 Integration of CTI Data Feeds

provide insights into security incidents or vulnerabilities that could affect IT service delivery, allowing ITSM platforms to correlate service disruptions with known global security threats.

3.14 Service Category 13: Vulnerability Assessment and Management:

Vulnerability Assessment and Management Solutions must enable organizations to continuously scan their IT assets for security vulnerabilities, evaluate the risks associated with these vulnerabilities, and prioritize remediation efforts. The Solution should automate both scanning and remediation workflows, providing real-time visibility into the organization's security posture.

The Service Category 13: Vulnerability Assessment and Management should provide:

3.14.1 Automated and Continuous Vulnerability Scanning

Solution should include automated and continuous scanning of network devices, servers, endpoints, and applications. The scans should identify known vulnerabilities (e.g., CVEs), misconfigurations, and missing patches.

3.14.2 Risk-Based Vulnerability Prioritization

Solution should allow vulnerabilities to be sorted and ranked based on the criticality of the affected asset, the exploitability of the vulnerability, and the business impact. This helps organizations focus on high-priority issues that pose the most risk.

3.14.3 Remediation Workflows

Solution should integrate with IT service management (ITSM) systems, automatically creating tickets or work orders for IT teams to address vulnerabilities, track progress, and close issues once remediated.

3.14.4 Detailed Vulnerability Reports

Solution should include the ability to provide reports including information such as affected assets, severity ratings (e.g., CVSS scores), vulnerability descriptions, and recommended fixes.

3.14.5 Real-Time Insights and Trend Analysis

Solution should provide insights into the overall security posture, such as the number of open vulnerabilities, time-to-remediation, and patch compliance rates.

3.14.6 Integration with Patch Management Solutions

Solution should allow organizations to deploy patches to vulnerable systems directly from the platform.

3.14.7 Integration of CTI Data Feeds

Solution should enhance vulnerability prioritization by providing real-time threat intelligence on active exploitation campaigns, emerging threats, or vulnerabilities that are being specifically targeted by threat actors.

3.15 Service Category 14: Cybersecurity Threat Intelligence (CTI):

Cybersecurity Threat Intelligence (CTI) Solutions must aggregate threat data from multiple sources, analyze it to uncover emerging threats, and provide actionable intelligence to enhance security defenses. The Solution should integrate with an organization's existing security operations workflows, ensuring that threat intelligence is used to improve detection, prevention, and response efforts.

The Service Category 14: Cybersecurity Threat Intelligence (CTI) should provide:

3.15.1 Threat Data Aggregation

Solution should include open-source threat feeds, paid subscriptions, and proprietary sources. The platform should support integration with standards-based threat intelligence feeds such as STIX, TAXII, and others.

3.15.2 Threat Intelligence Platform (TIP)

Solution should consolidate and normalize threat data, making it easy to share actionable intelligence with internal teams or external partners on a platform that has the capability to integrate with the CTI Solution. The platform should provide support for enrichment, scoring, and threat actor profiling.

3.15.3 Real-Time Threat Alerts

Solution should notify Customer designated security teams of emerging threats relevant to their environment, such as new vulnerabilities, malware campaigns, or attack techniques in real time. Alerts should include contextual information such as indicators of compromise (IoCs), threat actor motivations, and recommended mitigations.

3.15.4 Custom Intel

Solution should include the ability to incorporate threat intelligence feeds and manual intelligence to include custom work/intel.

3.15.5 Customer Feeds

Solution should include the ability to potentially change feeds if needed to include, remove, or modify research, analysis, and intelligence feeds.

3.15.6 Integration with SIEM, SOAR, and SOC Tools

Solution should provide contextual threat intelligence directly within the security operations workflow. This integration should enable automated response actions such as blocking malicious IP addresses or adjusting firewall rules based on threat intelligence.

3.15.7 Feed Control

Solution should include Capabilities for incorporating premium feeds and manual intelligence.

3.15.8 Dynamic Threat Detection

Solution should include the ability to provide tailored threat intelligence focusing on specific threats relevant to an organization's unique environment, including industry-specific and organization specific risks and potential adversaries, ensuring that security measures are aligned with real-world scenarios.

3.15.9 Threat Context

Solution should include the ability to provide contextual awareness threat intelligence, to include custom intelligence, that provides insights that consider the broader context of an organization's operations, including user behavior, network architecture, and business priorities, allowing for more informed risk management.

3.15.10 Threat Insights

Solution should include capability to provide actionable insights from custom intelligence offering clear recommendations for mitigation, response strategies, and risk prioritization, empowering an organization to make informed decisions and improve their security posture effectively.

3.16 Service Category 15: Data Security:

Data Security Solutions are designed to protect sensitive information from unauthorized access, loss, or exfiltration. The Solution should monitor data in use, in motion, and at rest, enforcing data protection policies, and detecting any unauthorized attempts to access or share sensitive data. The Solution must integrate with existing security frameworks and support compliance requirements to ensure organizations meet their regulatory obligations.

The Service Category 15: Data Security should provide:

3.16.1 Data Discovery and Classification

Solution should automatically identify and classify sensitive data across the organization's infrastructure, including databases, file shares, cloud storage, and endpoint devices. The classification engine should apply tags based on predefined policies for data types such

as Personally Identifiable Information (PII), financial data, and intellectual property. Enable continuous data discovery to detect new or modified data that requires protection.

3.16.2 Data Loss Prevention (DLP)

Solution should monitor and block unauthorized sharing of sensitive data across multiple communication channels, including email, cloud services, USB devices, and other pathways. Ensure that sensitive data is protected from being copied or moved without proper authorization, with real-time monitoring and alerting capabilities.

3.16.3 Encryption

Solution should ensure that sensitive data is encrypted both at rest and in transit using strong encryption algorithms, such as AES-256. Encryption should be applied to all data stored within the environment and transmitted across the network, ensuring that unauthorized access to data remains unreadable.

3.16.4 User and Entity Behavior Analytics (UEBA)

Solution should analyze how users interact with sensitive data, detecting anomalous behaviors such as copying large amounts of data, accessing restricted files, or sharing data with unauthorized third parties. The Solution should use machine learning to identify insider threats and abnormal data access patterns before breaches occur.

3.16.5 Automated Incident Response

Solution should automate response mechanisms to prevent unauthorized actions, such as blocking sensitive data transfers, issuing alerts, or requiring additional authentication when policy violations are detected. Quarantine suspicious files, block access to certain data, or alert security teams in real-time when DLP policies are breached.

3.16.6 Audit Trails and Reporting

Solution should provide comprehensive audit trails of all data-related activities, including details of who accessed sensitive data, what actions were taken, and when. Generate detailed reports for compliance audits, security evaluations, and incident response investigations.

3.16.7 Compliance Management

Solution should integrate with compliance management platforms to help organizations meet regulatory requirements (e.g., GDPR, CCPA, HIPAA) and provide detailed reporting on data access and protection measures. Ensure organizations can map security controls to compliance frameworks and track any compliance gaps.

3.16.8 Data Catalog and Metadata Management

Solution should provide comprehensive data discovery, search, and metadata management across various data sources within the organization. Metadata management should include data definitions, lineage, quality metrics, and usage patterns to ensure full context for all data assets. Provide tools for data profiling to assess data quality, identify inconsistencies, and maintain data completeness.

3.16.9 Integration with Data Management Tools

Solution should provide seamless integration with ETL (Extract, Transform, Load) tools, data warehousing, and analytics platforms to streamline data processing workflows. Ensure scalability, enabling the Solution to handle large volumes of data and grow with the organization's evolving needs.

3.16.10 Master Data Management (MDM)

Solution should provide capabilities to create and maintain a single, consistent view of master data (e.g., customer, product, or supplier data) across the organization. Ensure high data quality through robust cleansing, deduplication, and validation tools, while supporting governance frameworks for data ownership and access control.

3.17 Service Category 16: Enterprise Security Log Management, Analytics, and Response:

Enterprise Security Log Management, Analytics, and Response consists of multiple components that support and provide enterprise security operations, including Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and backend capabilities for log collection, storage, aggregation and analytics. This service category enables organizations to monitor, detect, and respond to security threats and provide operational visibility across their technology infrastructure.

The Service Category 16: Data Security should provide:

3.17.1 Data Collection and Aggregation

Solution should gather log data from multiple sources, including endpoints, servers, and applications, centralizing them for analysis. It supports structured and unstructured log formats like Syslog and JSON and provides or integrates with cybersecurity analysis solutions (such as SIEM).

3.17.2 Long-Term Data Storage

Solution should provide scalable storage Solutions like data and security lakes and archiving to ensure long-term retention of logs for compliance purposes. This includes cloud and on-premises storage with secure, tamper-proof archiving. Options including long-term/cold storage should be available.

3.17.3 Security Event Correlation

Solution should provide real-time event correlation, detecting complex attacks and anomalies.

3.17.4 Big Data Engine

Solution should process and analyze large volumes of security data in real time. By leveraging distributed computing frameworks this component enables complex threat detection, pattern recognition, and predictive analytics across large data sets. Provide training data sets to reduce false alerts and optimize efficiency of the platform.

3.17.5 Microservices Architecture

Solution should provide a modular approach to security operations, allowing individual services (e.g., log collection, incident response, threat detection) to operate independently. This architecture ensures scalability and flexibility, allowing organizations to adapt to evolving security needs without overhauling the entire system.

3.17.6 Monitoring and Threat Detection

Solution should provide continuous real-time monitoring with customizable alerts and advanced analytics that identify threats using machine learning, AI, and behavioral

analysis. Integration with threat intelligence ensures proactive threat detection and enriched security alerts with additional threat intelligence.

3.17.7 Log Management

Solution should provide centralized or federated management of logs, enabling real-time indexing and analysis of security events. It ensures that logs are stored and managed according to compliance standards, with flexible retention policies.

3.17.8 Incident Response and Automation

Solution should automate responses, isolating compromised systems or blocking malicious activity based on predefined playbooks. Incident management tools provide a centralized view of security events from detection to resolution.

3.17.9 Case Management and Collaboration

Solution should track incidents through case management, documenting all actions taken for compliance. Collaboration tools ensure effective communication among security team members.

3.17.10 Analytics and Reporting

Solution should provide powerful tools for transforming raw security data into meaningful insights. Customizable dashboards and reports help security teams and decision-makers visualize security metrics, alerts, and trends in real time. End User integration allows the platform to connect with business intelligence (BI) tools for further analysis and reporting.

3.18 **Optional Add-On Services**

Only Add-on Services on the Price Proposal may be purchased with a Solution under a purchase order. Add-On Services without a corresponding price entry on the Price Proposal shall be free of charge and considered a Value-Added Service if included on a resultant purchase order. Suggested, but not required, Add-On Services or Value-Added Services include:

3.17.1 Implementation (Optional)

Support for the initial implementation and successful deployment of the Solution for the Customer, including initial training and integration with existing systems.

3.17.2 Managed Security Services (Optional)

Deploy and maintain managed security services to support Customers, particularly with advanced administration of the Solution to support cybersecurity and incident response.

3.17.3 Application Management (Optional)

Distribute and manage native applications, provide stand-alone management for applications on unmanaged devices and application and data containment, and differentiate or isolate personal and corporate data.

3.17.4 On-Going Training (Optional)

Include any Solution training.

3.19 **Value-Added Services**

Contractors may offer additional services which clearly exceed the minimum requirements and are within the scope of this Contract, at no additional cost to the Customer. If the

Contractor proposes value-added services in response to a Request for Quote and are accepted by the Customer, the value-added services shall become a requirement and be a part of the minimum service specifications contained in any resulting Purchase Order.

4. Request for a Quote Requirement

Customers shall issue a Request for Quote (RFQ) to all Contractors in the applicable Service Category. Prior to issuing an RFQ for Service Categories 6: Content Delivery Network, 7: Security Operations Platform, and Service Category 10: Secure Access Service Edge (SASE), state agencies within the Enterprise shall consult with FL[DS] at purchasing@digital.fl.gov to determine if the RFQ complies with the Enterprise Architecture, as those terms are defined in section 282.0041(15), F.S. State agencies within the Enterprise shall comply with Rule 60GG-5.002, F.A.C.

4.1 Customer Specific Scope of Work (SOW)

Customers may develop a Customer Specific SOW which establishes additional Customer specific preferences, other requirements, or minimum service levels. If applicable. Customers shall include the Customer Specific SOW in the RFQ issued to the Contractors in a Service Category, and the Customer SOW shall be incorporated into any purchase order or contract issued by the Customer. Customers are permitted to negotiate terms and conditions which supplement those contained in this Term Contract. The Customer SOW may include, but is not limited to, the following information:

- Service Category
- Customer-specific scope of work requirements/service level agreement
- Customer-specific payment terms
- Customer-specific financial consequences for non-performance
- Customer-specific terms and conditions
- Anticipated timeline for work to be performed
- Additional Contractor responsibilities
- Kick off meeting requirements
- Reporting requirements
- Implementation plan, if applicable
- Security agreements, if applicable
- FL[DS] consultation, if applicable

5. Punchout Catalog and Electronic Invoicing

The Contractor is encouraged to provide an MFMP punchout catalog. The punchout catalog provides an alternative mechanism for suppliers to offer the State access to Products awarded under the Term Contract. The punchout catalog also allows for direct communication between the MFMP eProcurement System and a supplier's Enterprise Resource Planning (ERP) system, which can reflect real-time Product inventory/availability information.

The punchout catalog enables, Florida buyer to "punch out" to a supplier's website. Using the search tools on the supplier's Florida punchout catalog site, the user selects the desired Products. When complete, the user exits the supplier's punchout catalog site and the shopping cart (full of Products) is "brought back" to MFMP. No orders are sent to a supplier when the user exits the supplier's punchout catalog site. Instead, the chosen Products are "brought back" to MFMP as line items in a purchase order. The user can then proceed through the normal workflow steps, which may include adding, deleting, and editing Products (i.e., line items) in the purchase order.

An order is not submitted to a supplier until the user approves and submits the purchase order, at which point the supplier receives an email with the order details.

The Contractor may supply electronic invoices in lieu of paper-based invoices for those transactions processed through MFMP. Electronic invoices may be submitted to the agency through one of the mechanisms as listed below:

1) EDI (Electronic Data Interchange)

This standard establishes the data contents of the Invoice Transaction Set (EDI 810) for use within the context of an Electronic Data Interchange (EDI) environment. This transaction set can be used for invoicing via the Business Network (formerly known as Ariba Network) for catalog and non-catalog goods and services.

2) PO Flip via BN

This online process allows Contractors to submit invoices via the BN for catalog and non-catalog goods and services. Contractors are able to create an invoice directly from their inbox in their BN account by simply "flipping" the PO into an invoice. This option does not require any special software or technical capabilities.

The Contractor warrants and represents that it is authorized and empowered to and hereby grants the State and the third-party provider of MFMP, a State contractor, the right and license to use, reproduce, transmit, distribute, and publicly display within MFMP. In addition, the Contractor warrants and represents that it is authorized and empowered to and hereby grants the State and the third-party provider the right and license to reproduce and display within MFMP the Contractor's trademarks, system marks, logos, trade dress, or other branding designation that identifies the products made available by the Contractor under the Contract.

6. MFMP Transaction Fee Report

The Contractor is required to submit complete monthly MFMP Transaction Fee Reports to the Department. Reports are due 15 calendar days after the end of each month. Information on how to submit MFMP Transaction Fee Reports online can be located at [Transaction Fee and Reporting / MFMP Vendors / MyFloridaMarketPlace / State Purchasing / Business Operations / Florida Department of Management Services - DMS](#). Assistance with transaction fee reporting is also available by email at feeprocessing@myfloridamarketplace.com or telephone at 866-FLA-EPRO (866-352-3776) from 8:00 a.m. to 6:00 p.m. Eastern Time.

7. Quarterly Sales Reports

Contract Quarterly Sales Reports. The Contractor shall submit Quarterly Sales Reports in the manner and format required by the Department within 30 calendar days after the close of each State fiscal quarter (the State's fiscal quarters close on September 30, December 31, March 31, and June 30).

The Quarterly Sales Report template can be found here: [Quarterly Sales Report Format / Vendor Resources / State Purchasing / Business Operations / Florida Department of Management Services - DMS \(myflorida.com\)](#). Initiation and submission of the most recent version of the Quarterly Sales Report posted on the DMS website is the responsibility of the Contractor without prompting or notification from the Department. Sales will be reviewed on a quarterly basis. If no sales are recorded in two consecutive quarters, the Contractor may be placed on probationary status, or the Department may terminate the Contract. Failure to provide the Quarterly Sales Report, or other reports requested by the Department, will result in the imposition of financial

consequences and may result in the Contractor being found in default and the termination of the Contract.

Quarter 1 – (July-September) – due 30 calendar days after the close of the period.

Quarter 2 – (October-December) – due 30 calendar days after the close of the period.

Quarter 3 – (January-March) – due 30 calendar days after the close of the period.

Quarter 4 – (April-June) – due 30 calendar days after the close of the period.

8. Certified and Minority Business Enterprises Reports

Upon Customer request, the Contractor shall report to each Customer spend with certified and other minority business enterprises in the provision of commodities or services related to the Customer orders. These reports shall include the period covered, the name, minority code, and Federal Employer Identification Number of each minority business utilized during the period; commodities and services provided by the minority business enterprise, and the amount paid to each minority business enterprise on behalf of the Customer.

9. Telemetry Data Reporting

9.1 State Agency Customers agree, as a condition of utilizing the Digital Security Solutions state term contract, to provide all relevant cybersecurity log data from the purchased Solution including, but not limited to, event logs, access logs, firewall logs, and other security-related logs, to the Florida Digital Service (FLDS) upon request. This data must be provided in a format specified by FLDS and must be transmitted securely. The State Agency Customer is also responsible for ensuring that data shared complies with applicable state and federal regulations regarding privacy and data protection. Any resulting Customer Purchase Order or Agreement shall not prohibit the selected Vendor from disclosing data as contemplated in section 9.2.

9.2 The Vendor agrees, as a condition of providing services under the Digital Security Solutions state term contract, to transmit cybersecurity log data generated, collected, or managed as part of the services delivered pursuant to a purchased Solution to the Florida Digital Service (FLDS) upon request. This data includes, but is not limited to, event logs, access logs, firewall logs, and any other logs relevant to the monitoring and management of cybersecurity threats. The Vendor must ensure that log data is formatted according to FLDS specifications and securely transmitted. The Vendor must also adhere to applicable state and federal regulations regarding privacy and data protection when sharing log data.

10. Ad Hoc Reports

The Department may require additional Term Contract sales information such as copies of purchase orders or ad hoc sales reports. The Contractor shall submit these documents and reports in the form acceptable to the Department within the timeframe specified by the Department.

11. Financial Consequences

The Department reserves the right to impose financial consequences when the Contractor fails to comply with the requirements of the Term Contract. The following financial consequences will apply for the Contractor's non-performance under the Term Contract. The Customer and the Contractor may agree to add additional Financial Consequences on an as-needed basis beyond those stated herein to apply to that Customer's resultant contract or purchase order. The State of Florida reserves the right to withhold payment or implement other appropriate remedies, such

as Term Contract termination or nonrenewal, when the Contractor has failed to comply with the provisions of the Term Contract. The Contractor and the Department agree that financial consequences for non-performance are an estimate of damages which are difficult to ascertain and are not penalties.

The financial consequences below will be paid and received by the Department of Management Services within 30 calendar days from the due date specified by the Department. These financial consequences below are individually assessed for failures over each target period beginning with the first full month or quarter of the Term Contract performance and every month or quarter, respectively, thereafter.

Deliverable	Performance Metric	Performance Due Date	Financial Consequence for Non-Performance
Contractor will timely submit complete Quarterly Sales Reports	All Quarterly Sales Reports will be submitted timely with the required information	Completed reports are due on or before the 30 th calendar day after the close of each State fiscal quarter	\$250 per day late
Contractor will timely submit complete MFMP Transaction Fee Reports	All MFMP Transaction Fee Reports will be submitted timely with the required information	Completed reports are due on or before the 15 th calendar day after the close of each month	\$100 per day late

Failure to timely provide Quarterly Sales Reports, transaction fee reports, or other reports as required will result in the imposition of financial consequences and repeated failures or non- payment of financial consequences owed under this Term Contract may result in the Contractor being found in default and the termination of the Term Contract.

No favorable action will be considered when Contractor has outstanding Term Contract Quarterly Sales Reports, MFMP Transaction Fee Reports, or any other documentation owed to the Department or Customer, to include fees / monies, that is required under this Term Contract.

12. Business Review Meetings

Both the Department and Customer reserve the right to schedule business review meetings, which Contractor shall attend either virtually or in person. The Department or Customer may specify the format or agenda for the meeting. At a minimum, the Business Review Meeting may include the following topics:

- a. Contract compliance.
- b. Contract savings (in dollar amount and cost avoidance)
- c. Spend reports by Customer
- d. Recommendations for improved compliance and performance

Exhibit C



ENTERPRISE STANDARD TERMS AND CONDITIONS

These Enterprise Standard Terms and Conditions set forth the terms and conditions regarding the administration of the Term Contract, including the provision of Products to Customers. Customer specific terms for purchases off this Term Contract shall be set forth in the Customer specific agreement.

SECTION 1. DEFINITIONS

Capitalized terms used herein are defined as follows:

“Attachments” means the attachments, addenda, schedules, exhibits, and other documents, however so titled, attached hereto or incorporated by reference herein.

“Business Days” means Monday through Friday, inclusive, excluding State holidays specified in section 110.117, Florida Statutes (“F.S.”).

“Contractor” means the person or entity that is a party to the Term Contract and is offering Products for purchase.

“Customer” means 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.”), that makes a purchase off the Term Contract. For the avoidance of doubt, this also includes the Department when it purchases off the Term Contract.

“Department” means the Department of Management Services, an agency as defined in section 287.012, F.S., responsible for the administration of this Term Contract.

“Enterprise Alternate Contract Source” means a contract authorized pursuant to section 287.042(16), F.S., or approved pursuant to section 287.057(3)(b), F.S., for statewide use.

“Product” means any deliverable under the Term Contract, which may include commodities and contractual services, as each is defined in section 287.012, F.S. “Product” does not include, and no State funding under the Term Contract is being provided for, promoting, advocating for, or providing training or education on “Diversity, Equity, and Inclusion” (“DEI”). DEI is any program, activity, or policy that classifies individuals on the basis of race, color, sex, national origin, gender identity, or sexual orientation and promotes differential or preferential treatment of individuals on the basis of such classification, or promotes the position that a group or an individual’s action is inherently, unconsciously, or implicitly biased on the basis of such classification.

“State” means the State of Florida

“State Term Contract” means a term contract that is competitively procured by the department pursuant to section 287.057, F.S. and that is used by agencies and eligible users pursuant to section 287.056, F.S.

“Term Contract” means the legally enforceable term contract, as defined in section 287.012, F.S., between the Department and Contractor to which these Enterprise Standard Terms and Conditions apply, including all Attachments thereto. The Term Contract is either a State Term Contract or an Enterprise Alternate Contract Source.

SECTION 2. CONTRACT AMENDMENT

2.1 Amendment. The Term Contract contains all the terms and conditions agreed upon by the parties. Unless otherwise stated in Term Contract, the Term Contract may only be amended upon mutual written agreement signed by the parties. No oral agreements or representations will be valid or binding upon the Department or the Contractor. Unless explicitly agreed to by the Department in the Term Contract, no unilateral alteration or modification of the Term

Contract terms, including substitution of Product, will be valid or binding against the Customer.

The Department and Contractor may modify the Term Contract to alter, add to, or deduct from the Term Contract specifications, provided that such changes are within the general scope of the Term Contract. The parties may make an equitable adjustment in the Term Contract price or delivery date if the change affects the cost or time of performance.

SECTION 3. CONTRACT CONSTRUCTION AND ADMINISTRATION

3.1 Construction. Unless the context requires otherwise, (i) the words "include," "includes," and "including" are deemed to be followed by the words "without limitation;" (ii) the word "or" is not exclusive; and (iii) the words "herein," "hereof," "hereby," "hereto," and "hereunder" refer to the Term Contract as a whole, inclusive of all Attachments. Unless the context requires otherwise, references herein to (i) sections or Attachments mean the sections of, or Attachments to, the Term Contract; (ii) an agreement, instrument, or other document means such agreement, instrument, or other document as amended, supplemented, and modified from time to time to the extent permitted by the provisions thereof; and (iii) a statute, rule, or other law or regulation means such statute, rule, or other law or regulation as amended from time to time and includes any successor legislation thereto and any regulations promulgated thereunder.

Unless the context requires otherwise, whenever the masculine is used in the Term Contract, the same will include the feminine and whenever the feminine is used herein, the same will include the masculine. Unless the context requires otherwise, whenever the singular is used in the Term Contract, the same will include the plural, and whenever the plural is used herein, the same will include the singular, where appropriate. All references to "\$" or "dollars" means the United States Dollar, the official and lawful currency of the United States of America.

The Term Contract will be construed without regard to any presumption or rule requiring construction or interpretation against the party drafting an instrument or causing any instrument to be drafted. The Attachments referred to herein will be construed with, and as an integral part of, the Term Contract to the same extent as if they were set forth verbatim herein.

3.2 Administration. Execution in Counterparts. The Term Contract may be executed in counterparts, each of which will be an original and all of which will constitute but one and the same instrument.

3.2.1 Notices. Where the term "written notice" is used to specify a notice requirement herein, said notice will be deemed to have been given (i) when personally delivered; (ii) email (with confirmation of receipt) the day immediately following the day (except if not a Business Day then the next Business Day) on which the notice or communication has been provided prepaid by the sender to a recognized overnight delivery service; or (iii) on the date actually received except where there is a date of the certification of receipt.

Unless otherwise specified, the Contractor shall deliver all notices to the Department's Contract Manager and the Department shall deliver all notices to the Contractor's Contract Manager.

3.2.2 **Severability.** If a court deems any non-material provision of the Term Contract void or unenforceable, all other provisions will remain in full force and effect. Upon a determination that any material provision is void or unenforceable, the parties shall negotiate in good faith to modify this Term Contract to give effect to the original intent of the parties as closely as possible in order that the transactions contemplated hereby are consummated as originally contemplated to the greatest extent possible.

3.2.3 **Waiver.** The delay or failure by the Department to exercise or enforce any of its rights under the Term Contract will not constitute or be deemed a waiver of the Department's right thereafter to enforce those rights, nor will any single or partial exercise of any such right preclude any other or further exercise thereof or the exercise of any other right.

3.2.4 **Survivability.** The Term Contract and any and all promises, covenants, and representations made herein are binding upon the parties hereto and any and all respective heirs, assigns, and successors in interest. The respective obligations of the parties, which by their nature would continue beyond the termination or expiration of the Term Contract, including without limitation, the obligations regarding confidentiality, proprietary interests, reporting, and public records, will survive termination or expiration of the Term Contract.

3.2.5 **Third Party Beneficiaries.** The parties acknowledge and agree that the Term Contract is for the benefit of the parties hereto. The Term Contract is not intended to confer any legal rights or benefits on any other party, except such rights and benefits associated with a purchase made by a Customer off this Term Contract.

SECTION 4. CONTRACT TERM, SUSPENSION, AND TERMINATION.

4.1 **Term.** The initial term will begin on the date set forth in the Term Contract documents or on the date the Term Contract is signed by all parties, whichever is later.

Upon written agreement, the Department and the Contractor may renew the Term Contract in whole or in part only as set forth in the Term Contract documents, and in accordance with section 287.057(13), F.S. No costs may be charged for the renewals.

4.2 Suspension of Work and Termination.

4.2.1 **Suspension of Work.** The Department may, in its sole discretion, suspend any or all activities under the Term Contract, at any time, when it is in the best interest of the State of Florida to do so. The Department will provide the Contractor written notice outlining the particulars of the suspension. After receiving a suspension notice, the Contractor must comply with the notice and will cease the performance of the Term Contract. Suspension of work will not entitle the Contractor to any compensation for services not performed or commodities not delivered during the suspension period nor for any additional compensation.

4.2.2 **Termination for Convenience.** The Term Contract may be terminated by the Department, by written notice to the Contractor thirty (30) calendar days in advance, in whole or in part at any time, when the Department determines in its sole discretion that it is in the Department's interest to do so. The Contractor shall not furnish any Product after it receives the notice of termination, except as necessary to complete

the continued portion of the Term Contract, or a continued purchase off the Term Contract, if any. The Contractor will not be entitled to recover any cancellation charges or lost profits. If the Term Contract is terminated before performance is completed, the Contractor will 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 any Customer contract price as the amount of work satisfactorily performed. All work in progress will become the property of the Customer and will be turned over promptly by the Contractor.

- 4.2.3 **Termination for Cause.** The Department may terminate the Term Contract if the Contractor fails to (i) on multiple occasions, timely deliver Products purchased by Customers, (ii) on multiple occasions, maintain adequate progress on Customer purchases, thus endangering performance, (iii) honor any term of the Term Contract, or (iv) abide by any statutory, regulatory, or licensing requirement. The Department may, at its sole discretion, (i) immediately terminate the Term Contract, (ii) notify the Contractor of the deficiency and require that the deficiency be corrected within a specified time, otherwise the Term Contract will terminate at the end of such time, or (iii) take other action deemed appropriate by the Department. The Contractor shall continue work on any work not terminated.

Except for defaults of subcontractors at any tier, the Contractor will not be liable for any excess costs if the failure to perform arises from events completely beyond the control, and without the fault or negligence, of the Contractor. If the failure to perform is caused by the default of a subcontractor at any tier, and if the cause of the default is completely beyond the control of both the Contractor and the subcontractor, and without the fault or negligence of either, the Contractor will not be liable for any excess costs for failure to perform, unless the subcontracted Products were obtainable from other sources in sufficient time for the Contractor to meet the required delivery schedule. If, after termination, it is determined that the Contractor was not in default, or that the default was excusable, the rights and obligations of the parties will be the same as if the termination had been issued for the convenience of the Department. The rights and remedies of the Department in this clause are in addition to any other rights and remedies provided by law or under the Term Contract. The Customer will notify the Department of any vendor that has met the grounds for placement of the vendor on the Department of Management Services' Suspended Vendor List, as required in section 287.1351, F.S.

- 4.2.4 **Termination for Non-Compliance with E-Verify.** Pursuant to section 448.095(5)(c)1., F.S., the Department shall terminate the Term Contract if it has a good faith belief that the Contractor has knowingly violated section 448.09(1), F.S. Pursuant to section 448.095(5)(c)2., F.S., if the Department has a good faith belief that a subcontractor knowingly violated section 448.09(1), F.S., the Department shall promptly notify the Contractor and order the Contractor to immediately terminate the contract with the subcontractor.
- 4.2.5 **Termination Related to Statutory Certifications.** At the Department's option, the Term Contract may be terminated if the Contractor is placed on any of the lists referenced in the attached PUR 7801, Vendor Certification Form, or would otherwise be prohibited from entering into or renewing the Term Contract based on the statutory provisions referenced therein.

- 4.2.6 **Termination for Refusing Access to Public Records.** In accordance with section 287.058, F.S., the Department may unilaterally terminate the Term Contract for refusal by the Contractor to allow public access to all documents, papers, letters, or other material made or received by the Contractor in conjunction with the Term Contract, unless the records are exempt from s. 24(a) of Art. I of the State Constitution and section 119.071(1), F.S.

SECTION 5. PURCHASES OFF THE TERM CONTRACT.

- 5.1 Purchases.** By executing the Term Contract, the Contractor agrees to allow Customers to make purchases off the Term Contract. Purchases from Customers other than the Department are independent of the agreement between the Department and the Contractor, and the Department shall not be a party to such transaction. Customers' purchases off the Term Contract are limited to Products offered under the Term Contract, and no additional Products may be provided under a purchase off the Term Contract.
- 5.2 Purchase Submission.** For any purchases off the Term Contract, either the contract (as defined in Rule 60A-1.001, F.A.C.) must be executed between the Customer and Contractor, or the purchase order (as defined in Rule 60A-1.001, F.A.C.) must be issued by the Customer to the Contractor, no later than the last day of the Term Contract's term to be considered timely. Contracts executed, or purchase orders issued, after the last day of the Term Contract's term shall be considered void.
- 5.3 Terms.** The terms of the Form PUR 1000, General Contract Conditions, incorporated in Rule 60A-1.002, F.A.C., and linked here <http://www.flrules.org/Gateway/reference.asp?No=Ref-16731>, are hereby incorporated by reference herein and will apply to all purchases made by a Customer off the Term Contract. The Customer may attach additional terms and conditions specific to its particular purchase made off the Term Contract, which are considered Special Conditions. The term "Special Conditions" does not include any Contractor-provided documents, including attachments or standard preprinted forms, service agreements, end user agreements, product literature, or "shrink wrap" terms accompanying or affixed to a Product, whether written or electronic, or terms incorporated onto the Contractor's order or fiscal forms or other documents forwarded by the Contractor for payment. Any Customer Special Conditions shall not become a part of the Term Contract.
- 5.3.1 Term.** The term of the Customer purchase off the Term Contract will be as specified in the purchase, except that if renewals of the purchase are permitted, the Customer and Contractor shall not renew the purchase if the Term Contract expires prior to the effective date of the renewal. Any existing term of a purchase off the Term Contract shall not extend more than forty-eight (48) months beyond the end of the Term Contract. However, if an extended pricing plan offered in the Term Contract is agreed upon by the Customer and Contractor and extends more than forty-eight (48) months beyond the end of the Term Contract, the agreed upon extended pricing plan terms shall govern the maximum duration of the purchase. The Contractor is required to fulfill timely purchases that extend performance beyond the Term Contract term even when such extended delivery will occur after expiration of the Term Contract. For such purchases, all terms and conditions of the Term Contract shall survive the termination or expiration of the Term Contract and apply to the Contractor's continued performance.
- 5.3.2 Additional Requirements.** All Customer purchases off the Term Contract shall

contain the Term Contract name and number and shall be placed by the Customer. Delivery or furnishing Products shall not occur until the Customer executes their contract or transmits the purchase order, as defined in Rule 60A-1.001, F.A.C.

SECTION 6. PAYMENT AND FEES.

6.1 Pricing. The Contractor shall not exceed the pricing set forth in the Term Contract documents.

6.2 Best Pricing Offer. During the term of the Term Contract, if the Department or Customer becomes aware of better pricing offered by the Contractor for substantially the same or a smaller quantity of a Product outside the Term Contract, but upon the same or similar terms of the Term Contract, then the Department or Customer may request that the Contractor immediately reduce to the lower price.

6.3 Price Decreases. The following price decrease terms will apply to the Term Contract:

6.3.1 Quantity Discounts. The Contractor may offer additional discounts for one-time delivery of large single orders. The Customer should seek to negotiate additional price concessions on quantity purchases of any Products offered under the Term Contract.

6.3.2 Sales Promotions. In addition to decreasing prices for the balance of the Term Contract term due to a change in market conditions, the Contractor may conduct sales promotions involving price reductions for a specified lesser period. If conducting a sales promotion, the Contractor must submit documentation to the Department's Contract Manager identifying the proposed: (1) starting and ending dates of the promotion, (2) Products involved, and (3) promotional prices compared to then-authorized prices. The Contractor shall provide notice to Customers of the promotion and shall make the promotional prices available to all Customers.

6.3.3 Equitable Adjustment. The Department may, in its sole discretion, make an equitable adjustment in the Term Contract terms or pricing if pricing or availability of supply is affected by extreme and unforeseen volatility in the marketplace, that is, by circumstances that satisfy all the following criteria: (1) the volatility is due to causes wholly beyond the Contractor's control, (2) the volatility affects the marketplace or industry, not just the particular Term Contract source of supply, (3) the effect on pricing or availability of supply is substantial, and (4) the volatility so affects the Contractor that continued performance of the Term Contract would result in a substantial loss.

6.4 Purchase Prerequisites. The Contractor may be required to accept the State of Florida Purchasing Card and MyFloridaMarketPlace (MFMP) purchase orders. The Contractor must ensure that entities receiving payment directly from Customers under this Term Contract must have met the following requirements:

- Have an active registration with the Florida Department of State, Division of Corporations (www.sunbiz.org), or, if exempt from the registration requirements, provide the Department with the basis for such exemption.
- Be registered in the MFMP Vendor Information Portal (<https://vendor.myfloridamarketplace.com>).
- Have a current W-9 filed with the Florida Department of Financial Services (<https://flvendor.myfloridacfo.com>)

6.5 Transaction Fees. The State of Florida, through the Department of Management Services,

has instituted MyFloridaMarketPlace, a statewide eProcurement system pursuant to section 287.057(24), Florida Statutes (F.S.). All payments issued by Agencies to registered vendors for purchases of Commodities or Contractual Services under Chapter 287, F.S., shall be assessed the Transaction Fee of one percent (1.0%) of the total amount of the payments received from the State or Eligible Users, as prescribed by Rule 60A-1.031, Florida Administrative Code (F.A.C.), or as may otherwise be established by law. Vendors shall pay the Transaction Fee and are subject to automatic deduction of the Transaction Fee, when automatic deduction becomes available. Vendors shall submit any monthly reports required pursuant to Rule 60A-1.031, F.A.C. All such reports and payments are subject to audit. The Agency will have grounds for declaring the vendor in default if the vendor fails to comply with the payment of the Transaction Fee or reporting of payments, which may subject the vendor to being suspended from business with the State of Florida.

- 6.6 Exclusivity.** The Term Contract is not an exclusive license to provide the Products described in the Term Contract. The Department may, without limitation and without recourse by the Contractor, contract with other vendors to provide the same or similar Products.

SECTION 7. PERFORMANCE

- 7.1 Warranty of Ability to Perform.** Upon the effective date of the Term Contract, and each year on the anniversary date of the Term Contract, the Contractor shall submit to the Department a completed PUR 7801, Vendor Certification Form. The Contractor warrants that, to the best of its knowledge, there is no pending or threatened action, proceeding, or investigation, or any other legal or financial condition, that would in any way prohibit, restrain, or diminish the Contractor's ability to satisfy its Term Contract obligations.

Additionally, the Contractor shall promptly notify the Department in writing if its ability to perform is compromised in any manner during the term of the Term Contract (including potential inability to renew the Term Contract due to section 287.138 or 908.111, F.S.) or if it or its suppliers, subcontractors, or consultants under the Term Contract are placed on the Suspended Vendor, Convicted Vendor, Discriminatory Vendor, Forced Labor Vendor, or Antitrust Violator Vendor Lists. The Contractor shall use commercially reasonable efforts to avoid or minimize any delays in performance and shall inform the Department of the steps the Contractor is taking or will take to do so, and the projected actual completion (or delivery) time. If the Contractor believes a delay in performance by the Department has caused or will cause the Contractor to be unable to perform its obligations on time, the Contractor shall promptly so notify the Department and use commercially reasonable efforts to perform its obligations on time notwithstanding the Department's delay.

- 7.2 Further Assurances.** The parties shall, with reasonable diligence, do all things and provide all reasonable assurances as may be necessary to complete the requirements of the Term Contract, and each party shall provide such further documents or instruments requested by the other party as may be reasonably necessary or desirable to give effect to the Term Contract and to carry out its provisions. The Department is entitled at all times, upon request, to be advised as to the status of work being done by the Contractor and the details thereof.
- 7.3 Assignment.** The Contractor shall not sell, assign or transfer any of its rights, duties or obligations under the Term Contract without the prior written consent of the Department. In the event of any assignment, the Contractor remains secondarily liable for performance of

the Term Contract, unless the Department expressly waives such secondary liability. The Department may assign the Term Contract with prior written notice to Contractor of its intent to do so.

7.4 Employees, Subcontractors, and Agents.

7.4.1 **Subcontractors.** The Contractor will not subcontract any work under the Term Contract without prior written consent of the Department. The Contractor shall obtain prior written consent using the process identified on the Department's website: [Subcontractor/Dealer/Reseller Forms / Vendor Resources / State Purchasing / Business Operations - Florida Department of Management Services \(myflorida.com\)](https://myflorida.com/contractors/subcontractor-dealer-reseller-forms/). The use of the term "subcontractor" may refer to affiliates, resellers, dealers, distributors, partners, teammates, and all other third parties utilized by the Contractor at any tier under the Term Contract. The Contractor is responsible for ensuring that its subcontractors providing commodities and performing services in furtherance of the Term Contract do so in compliance with the terms and conditions of the Term Contract. By execution of the Term Contract, the Contractor acknowledges that it will not be released of its contractual obligations to Customers because of any failure of a subcontractor. The Contractor is fully responsible for satisfactory completion of all work performed under the Term Contract. The Contractor's use of a subcontractor not approved by the Department will be considered a material breach of the Term Contract.

7.4.2 **Independent Contractor.** The Contractor and its employees, agents, representatives, and subcontractors are not employees or agents of the Department or the State and are not entitled to the benefits of Department or State employees. Neither the Customer nor the State will be bound by any acts or conduct of the Contractor or its employees, subcontractors, or agents. The Contractor shall include this provision in all of its subcontracts under the Term Contract.

7.5 Force Majeure, Notice of Delay, and No Damages for Delay. The Contractor will not be responsible for delay resulting from its failure to perform if neither the fault nor the negligence of the Contractor or its employees, subcontractors, or agents contributed to the delay and the delay is due directly to acts of God, wars, acts of public enemies, strikes, fires, floods, or other similar cause wholly beyond the Contractor's control, or for any of the foregoing that affect suppliers if no alternate source of supply is available to the Contractor.

In case of any delay the Contractor believes is excusable, the Contractor shall notify the Department in writing of the delay or potential delay and describe the cause of the delay either (i) within ten (10) calendar days after the cause that creates or will create the delay first arose, if the Contractor could reasonably foresee that a delay could occur as a result; or (ii) if a delay is not reasonably foreseeable, within five (5) calendar days after the date the Contractor first had reason to believe that a delay could result. THE FOREGOING WILL CONSTITUTE THE CONTRACTOR'S SOLE REMEDY OR EXCUSE WITH RESPECT TO ANY DELAY except if such delay is caused by the fraud, bad faith, or active interference of the Department. Providing notice in strict accordance with this paragraph is a condition precedent to such remedy, and a rebuttable presumption of prejudice will exist based on Contractor's untimely notice. The Contractor shall not assert any claim for damages related to such delay. The Contractor will not be entitled to an increase in the Term Contract price or payment of any kind from the Department for direct, indirect, consequential, impact, or other costs, expenses, or damages, including costs of acceleration or inefficiency, arising

because of delay, disruption, interference, or hindrance from any cause whatsoever.

If performance is suspended or delayed, in whole or in part, due to any of the causes described in this subsection, the Department may unilaterally (and with no recourse on the part of the Contractor) identify and use an alternate source to complete any work under the Term Contract as the Department deems necessary, in its sole discretion. After the causes have ceased to exist, the Contractor shall perform at no increased cost, unless the Department determines, in its sole discretion, that the delay will significantly impair the value of the Contract to the Department or State, in which case the Department may (i) accept allocated performance or deliveries from the Contractor, provided that the Contractor grants preferential treatment to the Department with respect to Products subjected to allocation; or (ii) terminate the Term Contract in whole or in part.

SECTION 8. CONTRACT MANAGEMENT

8.1 Department's Contract Manager. The Department's Contract Manager for the Term Contract, who is primarily responsible for the Department's oversight of the Term Contract, will be identified in a separate writing to the Contractor upon Term Contract signing in the following format:

Department's Contract Manager Name
 Department's Name
 Department's Physical Address
 Department's Telephone #
 Department's Email Address

8.2 Contractor's Contract Manager. The Contractor's Contract Manager, who is primarily responsible for the Contractor's oversight of the Term Contract performance, will be identified in a separate writing to the Department upon Term Contract signing in the following format:

Contractor's Contract Manager Name
 Contractor's Name
 Contractor's Physical Address
 Contractor's Telephone #
 Contractor's Email Address

Either party may notify the other by email of a change to a designated contact providing the contact information for the newly designated contact, and such notice is sufficient to effectuate this change without requiring a written amendment to the Term Contract.

SECTION 9. COMPLIANCE WITH LAWS.

9.1 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 and that are applicable to the Term Contract, including those of federal, state, and local agencies having jurisdiction and authority, and shall ensure that any and all subcontractors utilized do the same. The Contractor represents and warrants that no part of the funding under the Term Contract will be used in violation of any state or federal law, including, but not limited to, 8 U.S.C. § 1324 or 8 U.S.C. § 1325, or to aid or abet another in violating state or federal law. The Department may terminate the Term Contract at any time if the Contractor violates, or aids or abets another in violating, any state or federal law.

If the requirements of the Term Contract conflict with any governing law, codes or regulations, the Contractor shall notify the Department in writing and the parties shall amend the Term Contract to comply with the applicable code or regulation. Similarly, if the Contractor believes that any governmental restrictions have been imposed that require alteration of the material, quality, workmanship or performance of the Products offered under the Term Contract, the Contractor shall immediately notify the Department in writing, indicating the specific restriction. The Department reserves the right and the complete discretion to accept any such alteration or to cancel the Term Contract at no further expense to the Department.

Pursuant to section 287.057(26), F.S., the Contractor shall answer all questions of, and ensure a representative will be available to, a Customer's continuing oversight team for purchases off this Term Contract.

9.2 Integrity. In addition to any applicable statutory restrictions, the Contractor shall not, in connection with this or any other agreement with the State, directly or indirectly (i) offer, confer, or agree to confer any pecuniary benefit on 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 (ii) offer, give, or agree to give to anyone any gratuity for the benefit of, or at the direction or request of, any State officer or employee. For purposes of clause (ii), "gratuity" means any payment in the form of cash, travel, entertainment, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind.

SECTION 10. DISPUTES AND LIABILITIES.

10.1 Dispute Resolution. Should any disputes arise between the Department and the Contractor with respect to the Term Contract, the Contractor and the Department shall act immediately to resolve any such disputes. Time is of the essence in the resolution of disputes.

Exhaustion of this administrative remedy detailed in the Dispute Resolution Process contemplated in this Term Contract is an absolute condition precedent to the Contractor's ability to seek other remedies related to the Term Contract.

10.2 Dispute Resolution Process.

- (a) Department Review. The parties shall resolve disputes through written submission of their dispute to the Department's Contract Manager. The Department shall respond to the dispute in writing within ten (10) Business Days from the date that the Department's Contract Manager receives the dispute. The Department's decision shall be final unless a party provides the other party with written notice of the party's disagreement with the decision within ten (10) Business Days from the date of the Department's decision. If a party disagrees with the Department's decision, the party may proceed to subsection (b) below.
- (b) Meeting between the Principals. If either party disagrees with the Department's decision, such disagreeing party shall notify the other party of the disagreement within ten (10) Business Days. The parties shall then schedule a meeting between each party's principal (for the Department, the Department head or designee; for the Contractor, the Chief Executive Officer or designee) on a mutually agreed upon date, no later than ten (10) Business Days after the provision of the notice. The principals shall attempt to mutually resolve the disagreement at such meeting.
- (c) Mediation. If the dispute is not resolved through a meeting of the Principals, the parties, upon mutual agreement, may mediate such dispute. If such mediation is not completed

within 100 calendar days from receipt of the Department's decision, then either party may seek other remedies.

If the dispute is not resolved through the full process in subsections (a) - (c) above (or (a) – (b), if mediation is not agreed to), either party may pursue any other remedies.

10.3 Contractor's Obligation to Perform While Disputes are Pending. The Contractor shall proceed diligently with performance under the Term Contract pending the final resolution of any dispute or request for relief, claim, appeal, or action arising under the Term Contract and shall comply with directions to perform from the Department. Should the Contractor not perform while a dispute is pending, including by not performing disputed work, such nonperformance by the Contractor may be deemed to be an unexcused breach of the Term Contract which is separate and apart from any other dispute.

10.4 Governing Law and Venue. The Term Contract will be governed by, and construed in accordance with, the laws of the State. Jurisdiction and venue for suit arising under the terms of the Term Contract will exclusively be in the appropriate State court located in Leon County, Florida. Except as otherwise provided by law, the parties agree to be responsible for their own attorney's fees and costs incurred in connection with disputes arising under the terms of the Term Contract.

10.5 Remedies Cumulative. No remedy herein conferred upon or reserved to either party is intended to be exclusive of any other remedy or remedies, and each and every such remedy will be cumulative, and will be in addition to every other remedy given hereunder or now or hereafter existing at law or in equity.

10.6 JURY WAIVER. THE PARTIES, ON BEHALF OF THEMSELVES AND ASSIGNS, WAIVE ALL RIGHT TO TRIAL BY JURY FOR ANY ACTION, APPEAL, CLAIM, OR PROCEEDING, WHETHER IN LAW IN OR IN EQUITY, WHICH IN ANY WAY ARISES OUT OF OR RELATES TO THE TERM CONTRACT OR ITS SUBJECT MATTER.

10.7 Indemnification. For any and all third-party claims, actions, demands, liabilities, and expenses of any kind which are caused by, related to, growing out of or happening in connection with the Term Contract (including any determination arising out of or related to the Term Contract that the Contractor or its employees, agents, subcontractors, assignees, or delegates are not independent contractors in relation to the Department or State), the Contractor shall be fully liable for the actions of its employees, subcontractors, and agents and shall fully indemnify, defend, and hold harmless the Department and the State (including each of their current and former officers, agents, and employees) for any and all loss, damage, injury, costs, reasonable expenses, or other casualty to person or property. Without limiting this indemnification requirement, the Department may provide the Contractor (i) written notice of any action or threatened action, (ii) the opportunity to take over and settle or defend any such action at the Contractor's sole expense, and (iii) assistance in defending the action at the Contractor's sole expense. The above indemnity requirement does not apply to that portion of any loss or damages proximately caused by the negligent act or omission of the Department or the State. Nothing herein is intended to act as a waiver of the Department's or State's sovereign immunity or to be deemed consent by the Department or State or its subdivisions to suit by third parties.

SECTION 11. MISCELLANEOUS.

- 11.1 Department of State Registration.** Consistent with Title XXXVI, F.S., if the Contractor asserts status other than that of a sole proprietor, it must provide the Department with i) conclusive evidence of a certificate of status, not subject to qualification, if a Florida business entity; ii) a certificate of authorization if a foreign business entity; or iii) if exempt from the registration requirements, a basis for such exemption.
- 11.2 Time is of the Essence.** Time is of the essence regarding every obligation of the Contractor under the Term Contract. Each obligation is deemed material, and a breach of any such obligation (including a breach resulting from untimely performance) is a material breach.
- 11.3 Cooperative Purchasing.** Pursuant to their own governing laws, and subject to the agreement of the Contractor, governmental entities that are not Customers may make purchases under the terms and conditions contained herein, if agreed to by the Contractor. Such purchases are independent of the Term Contract between the Department and the Contractor, and the Department is not a party to these transactions.

SECTION 12. PUBLIC RECORDS, TRADE SECRETS, DOCUMENT MANAGEMENT, AND INTELLECTUAL PROPERTY.

- 12.1 General Record Management and Retention.** The Contractor shall retain all records that were made in relation to the Term Contract for the longer of five (5) years after expiration of the Term Contract or the period required by the General Records Schedules maintained by the Florida Department of State available at: <https://dos.fl.gov/library-archives/records-management/general-records-schedules/>.
- 12.2 Identification and Protection of Confidential Information.** Article 1, section 24, of the Florida Constitution, guarantees every person access to public records, and section 119.011, F.S., provides a broad definition of “public record.” As such, records submitted to the Department (or any other State agency) are public records and are subject to disclosure unless exempt from disclosure by law. If the Contractor considers any portion of a record it provides to the Department (or any other State agency) to be trade secret or otherwise confidential or exempt from disclosure under Florida or federal law (“Confidential Information”), the Contractor shall mark as “confidential” each page of a document or specific portion of a document containing Confidential Information and simultaneously provide the Department (or other State agency) with a separate, redacted copy of the record. The Contractor shall state the basis of the exemption that the Contractor contends is applicable to each portion of the record redacted, including the specific statutory citation for such exemption. The Contractor shall only redact portions of records that it claims contains Confidential Information. If the Contractor fails to mark a record it claims contains Confidential Information as “confidential,” or fails to submit a redacted copy in accordance with this section of a record it claims contains Confidential Information, the Department (or other State agency) shall have no liability for release of such record. The foregoing will apply to every instance in which the Contractor fails to both mark a record “confidential” and redact it in accordance with this section, regardless of whether the Contractor may have properly marked and redacted the same or similar Confidential Information in another instance or record submitted to the Department (or any other State agency).

In the event of a public records request, to which records the Contractor marked as “confidential” are responsive to the request, the Department shall provide the Contractor-redacted copy to the requestor. If the Contractor has marked a record as “confidential” but

failed to provide a Contractor-redacted copy to the Department, the Customer may notify the Contractor of the request and the Contractor may have up to ten (10) Business Days from the date of the notice to provide a Contractor-redacted copy, or else the Department may release the unredacted record to the requestor without liability. If the Department provides a Contractor-redacted copy of the documents and the requestor asserts a right to the Contractor-redacted Confidential Information, the Department shall promptly notify the Contractor such an assertion has been made. The notice will provide that if the Contractor seeks to protect the Contractor-redacted Confidential Information from release it must, within thirty (30) days after the date of the notice and at its own expense, file a cause of action seeking a declaratory judgment that the information in question is exempt from section 119.07(1), F.S., or other applicable law and an order prohibiting the Department from publicly disclosing the information. The Contractor shall provide written notice to the Department of any cause of action filed. If the Contractor fails to file a cause of action within thirty (30) days the Department may release the unredacted copy of the record to the requestor without liability.

If the Department is requested or compelled in any legal proceeding to disclose documents that are marked as "confidential" (whether by oral questions, interrogatories, requests for information or documents, subpoena, or similar process), unless otherwise prohibited by law, the Department shall give the Contractor prompt written notice of the demand or request prior to disclosing any Confidential Information to allow the Contractor to seek a protective order or other appropriate relief at the Contractor's sole discretion and expense. If the Contractor fails to take appropriate and timely action to protect the Confidential Information contained within documents it has marked as "confidential" or fails to provide a redacted copy that may be disclosed, the Department may provide the unredacted records in response to the demand without liability.

The Contractor shall protect, defend, and indemnify the Department for all claims, costs, fines, settlement fees, and attorneys' fees, at both the trial and appellate levels, arising from or relating to the Contractor's determination that its records contain Confidential Information. In the event of a third-party claim brought against the Department for failure to release the Contractor's redacted Confidential Information, the Contractor shall assume, at its sole expense, the defense or settlement of such claim, including attorney's fees and costs at both the trial and appellate levels. If the Contractor fails to continuously undertake the defense or settlement of such claim or if the Contractor and Department mutually agree that the Department is best suited to undertake the defense or settlement, the Department will have the right, but not the obligation, to undertake the defense or settlement of such claim, at its discretion. The Contractor shall be bound by any defense or settlement the Department may make as to such claim, and the Contractor agrees to reimburse the Department for the expense, including reasonable attorney's fees and costs at both the trial and appellate levels associated with any defense or settlement that the Department may undertake to defend Contractor's Confidential Information. The Department will also be entitled to join the Contractor in any third-party claim for the purpose of enforcing any right of indemnity under this section.

If at any point the Department is reasonably advised by its counsel that disclosure of the Confidential Information is required by law, including but not limited to Florida's public records laws, the Department may disclose such Confidential Information without liability hereunder.

12.3 Public Records Requirements Pursuant to Section 119.0701, F.S. Solely for the purpose of this section, the Department's Contract Manager is the agency custodian of public records. If, under the Term Contract, the Contractor is providing services and is acting on behalf of the public agency, as provided in section 119.0701, F.S., the Contractor shall:

- i. Keep and maintain public records required by the Department to perform the service.
- ii. Upon request from the Department's custodian of public records, provide the Department with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law.
- iii. 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 Term Contract term and following the completion of the Term Contract if the Contractor does not transfer the records to the Department.
- iv. Upon completion of the Term Contract, transfer, at no cost, to the Department all public records in possession of the Contractor or keep and maintain public records required by the Department to perform the service. If the Contractor transfers all public records to the Department upon completion of the contract, 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 Term Contract, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the Department, upon request from the Department's custodian of public records, in a format that is compatible with the information technology systems of the Department.

IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS TERM CONTRACT, CONTACT THE DEPARTMENT'S CUSTODIAN OF PUBLIC RECORDS AT PUBLICRECORDS@DMS.FL.GOV, (850) 487-1082 OR 4050 ESPLANADE WAY, SUITE 160, TALLAHASSEE, FLORIDA 32399-0950.

12.4 Advertising. Subject to Chapter 119, Florida Statutes, the Contractor shall not publicly disseminate any information concerning the Term Contract without prior written approval from the Department, including mentioning the Term Contract in a press release or other promotional material, identifying the Department or the State as a reference, or otherwise linking the Contractor's name and either a description of the Term Contract or the name of the Department or the State in any material published, either in print or electronically, to any entity that is not a party to the Term Contract, except potential or actual Customers or authorized distributors, dealers, resellers, or service representatives.

12.5 Intellectual Property.

12.5.1 Ownership. Unless specifically addressed otherwise in the Customer's contract, the State of Florida shall be the owner of all intellectual property rights to all new property created or developed in connection with the Customer's contract. This shall not apply

to intellectual property developed prior to the execution of the Term Contract.

12.5.2 Patentable Inventions or Discoveries. Any inventions or discoveries developed in the course, or as a result, of services in connection with the Customer's contract that are patentable pursuant to 35 U.S.C. § 101 are the sole property of the State of Florida. Contractor must inform the Customer and the Department of any inventions or discoveries developed or made through performance of the Customer's contract, and such inventions or discoveries will be referred to the Florida Department of State for a determination on whether patent protection will be sought. The State of Florida will be the sole owner of all patents resulting from any invention or discovery made through performance of the Customer's contract. This shall not apply to any invention or discovery made prior to the execution of the Term Contract.

12.5.3 Copyrightable Works. Contractor must notify the Customer and the Department of any publications, artwork, or other copyrightable works developed in connection with the Customer's contract. All copyrights created or developed through performance of the Customer's contract are owned solely by the State of Florida. This shall not apply to any copyrightable works created or developed prior to the execution of the Term Contract.

SECTION 13. DATA SECURITY.

The Contractor will maintain the security of State of Florida data including, but not limited to, maintaining a secure area around any displayed visible data and ensuring data is stored and secured when not in use. "State of Florida data" means data collected by, transmitted from, created for, or provided by the Department or the Customer. The Contractor will not allow any State of Florida data to be sent by any medium, transmitted, or accessed outside the United States due to Contractor's action or inaction. In the event of a Security Incident involving State of Florida data, the Contractor shall give notice to the Customer and the Department within one business day of becoming aware of the Security Incident. "Security Incident" for purposes of this section will refer to an actual or imminent threat of a violation of information technology resources, security, policies, or practices, unauthorized access of State of Florida data, or occurrences that compromise the confidentiality, integrity, or availability of State of Florida data. An imminent threat refers to a situation in which the Contractor has a factual basis for believing that a specific incident is about to occur. Once a data breach has been contained, the Contractor must provide the Department and the Customer with a post-incident report documenting all containment, eradication, and recovery measures taken. The Department reserves the right in its sole discretion to enlist a third party to audit Contractor's findings and produce an independent report, and the Contractor will fully cooperate with the third party. The Contractor will also comply with all HIPAA requirements and any other current state and federal rules and regulations regarding security of information.

SECTION 14. CONTRACT MONITORING.

14.1 Performance Standards. The Contractor agrees to perform all tasks and provide deliverables as set forth in the Term Contract. The Customer will 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.

14.2 Contract Reporting. The Contractor shall provide the Department the following accurate and complete reports associated with this Term Contract.

- 14.2.1 **Term Contract Quarterly Sales Reports.** The Contractor shall submit Quarterly Sales Reports in the manner and format required by the Department within 30 calendar days after the close of each State fiscal quarter (the State's fiscal quarters close on September 30, December 31, March 31, and June 30).

The Quarterly Sales Report template can be found here: [Quarterly Sales Report Format / Vendor Resources / State Purchasing / Business Operations / Florida Department of Management Services - DMS \(myflorida.com\)](#). Initiation and submission of the most recent version of the Quarterly Sales Report posted on the DMS website is the responsibility of the Contractor without prompting or notification from the Department. Sales will be reviewed on a quarterly basis. If no sales are recorded in two consecutive quarters, the Contractor may be placed on probationary status, or the Department may terminate the Term Contract. Failure to provide the Quarterly Sales Report, or other reports requested by the Department, will result in the imposition of financial consequences and may result in the Contractor being found in default and the termination of the Term Contract.

- 14.2.2 **Certified and Minority Business Enterprises Reports.** Upon Customer request, the Contractor shall report to each Customer spend with certified and other minority business enterprises in the provision of commodities or services related to the Customer orders. These reports shall include the period covered; the name, minority code, and Vendor Identification Information of each minority business enterprise utilized during the period; commodities and services provided by the minority business enterprise; and the amount paid to each minority business enterprise on behalf of the Customer.

- 14.2.3 **Ad Hoc Sales Reports.** The Department may require additional Term Contract sales information such as copies of purchase orders or ad hoc sales reports. The Contractor shall submit these documents and reports in the format acceptable to the Department and within the timeframe specified by the Department.

- 14.2.4 **MFMP Transaction Fee Reports.** The Contractor shall submit complete monthly MFMP Transaction Fee Reports to the Department. Reports are due 15 calendar days after the end of each month. Information on how to submit MFMP Transaction Fee Reports online can be located at https://www.dms.myflorida.com/business_operations/state_myfloridamarketplace/mfmp_vendors/transaction_fee_and_reporting. Assistance with transaction fee reporting is also available by email at feeprocessing@myfloridamarketplace.com or telephone at 866-FLA-EPRO (866-352-3776) from 8:00 a.m. to 6:00 p.m. Eastern Time.

- 14.3 **Business Review Meetings.** Both the Department and Customer reserve the right to schedule business review meetings. The Department or Customer may specify the format or agenda for the meeting. At a minimum, the Business Review Meeting may include the following topics:

- Term Contract or Customer contract compliance
- Term Contract savings (in dollar amount and cost avoidance)
- Spend reports by Customer
- Recommendations for improved compliance and performance

14.4 Performance Deficiencies.

14.4.1 **Proposal of a Corrective Action Plan.** In addition to the processes set forth in the Term Contract (e.g., service level agreements), if the Customer or the Department determines that there is a performance deficiency that requires correction by the Contractor, then the Customer or the Department will notify the Contractor. The correction must be made within a timeframe specified by the Customer or the Department. The Contractor must provide the Customer or the Department with a corrective action plan describing how the Contractor will address all performance deficiencies identified by the Customer or the Department.

14.4.2 **Retainage for Unacceptable Corrective Action Plan or Plan Failure.** For Customer-requested Corrective Action Plans, if the corrective action plan is unacceptable to the Customer, or implementation of the plan fails to remedy the performance deficiencies, the Customer will retain ten percent (10%) of the total invoice amount. The retainage will be withheld until the Contractor resolves the performance deficiencies. If the performance deficiencies are resolved, the Contractor may invoice the Customer for the retained amount. If the Contractor fails to resolve the performance deficiencies, the retained amount will be forfeited to compensate the Customer for the performance deficiencies.

14.5 Inspection.

14.5.1 **Inspection at Contractor's Site.** The Department reserves the right to inspect, or enlist a third-party to perform, at any reasonable time with prior notice, the equipment, product, plant or other facilities of the Contractor to assess conformity with Term Contract requirements and to determine whether they are adequate and suitable for proper and effective Term Contract performance.

14.5.2 **Statutory Inspection Rights.** If services are to be provided pursuant to the Term Contract, in accordance with section 216.1366, F.S., the Department is authorized to inspect the: (i) financial records, papers, and documents of the Contractor that are directly related to the performance of the Term Contract or the expenditure of State funds; and (ii) programmatic records, papers, and documents of the Contractor which the Department determines are necessary to monitor the performance of the Term Contract or to ensure that the terms of the Term Contract are being met. The Contractor shall provide such records, papers, and documents requested by the Department within ten (10) Business Days after the request is made.

Further, for any Term Contract for services with a nonprofit organization as defined in section 215.97(2)(m), F.S., the Contractor must provide documentation that indicates the amount of state funds:

1. Allocated to be used during the full term of the Term Contract for remuneration to any member of the board of directors or an officer of the contractor; and
2. Allocated under each payment by the public agency to be used for remuneration of any member of the board of directors or an officer of the contractor.

The documentation must indicate the amounts and recipients of the remuneration.

14.5.3 Inspection Compliance. The Contractor understands its, and its subcontractors (if any), duty, pursuant to section 20.055(5), F.S., to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing. Upon request of the Department's Inspector General, or other authorized State official, the Contractor shall provide any type of information the State official deems relevant to the Contractor's integrity or responsibility. Such information may include the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Term Contract. 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 the Term Contract or any other agreement between the Contractor and the State which results in the suspension or debarment of the Contractor. Such costs will include salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor shall not be responsible for any costs of investigations that do not result in the Contractor's suspension or debarment.

SECTION 15. PERFORMANCE OR COMPLIANCE AUDITS.

The Department may conduct or have conducted performance and/or compliance audits of the Contractor and subcontractors as determined by the Department. The Department may conduct an audit and review all the Contractor's and subcontractors' data and records that directly relate to the Term Contract. To the extent necessary to verify the Contractor's fees and claims for payment under the Term Contract, the Contractor's agreements or contracts with subcontractors, partners, or agents of the Contractor, pertaining to the Term Contract, may be inspected by the Department upon fifteen (15) calendar days' notice, during normal working hours and in accordance with the Contractor's facility access procedures where facility access is required. Release statements from its subcontractors, partners, or agents are not required for the Department or its designee to conduct compliance and performance audits on any of the Contractor's contracts relating to this Term Contract.

SECTION 16. CONFIDENTIALITY.

The Contractor shall not divulge to third parties any confidential information obtained by the Contractor or its employees, subcontractors, or agents in the course of performing Term Contract work, including security procedures, business operations information, or commercial proprietary information in the possession of the Customer or State. The Contractor will not be required to keep confidential information or material that is publicly available through no fault of the Contractor, material that the Contractor developed independently without relying on the Customer's or State's confidential information, or material that is otherwise obtainable under State law as a public record. To ensure confidentiality, the Contractor shall take appropriate steps as to its employees, subcontractors, and agents.

SECTION 17. SUPPLIER DEVELOPMENT.

17.1 Office of Supplier Development. The State of Florida supports its business community by creating opportunities for business enterprises to participate in procurements and contracts. The Department encourages supplier development through certain certifications and provides advocacy, outreach, and networking through regional business events. For additional information, please contact the Office of Supplier Development (OSD) at OSDHelp@dms.fl.gov.

17.2 Reporting Certified Business Enterprises. Upon request, the Contractor will report to the Department its spend with business enterprises certified by the OSD. These reports must include the time period covered, the name and vendor identification information of each business enterprise utilized during the period, commodities and contractual services provided by the business enterprise, and the amount paid to the business enterprise on behalf of each agency purchasing under the Term Contract.