Department of MANAGEMENT SERVICES
We serve those who serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950
850-488-2786

Ron DeSantis, Governor
Jonathan R. Satter, Secretary

ATTACHMENT A – STATEMENT OF WORK

FOR

STATE DATA CENTER MANAGED SERVICE PROVIDER

ITN NO: DMS-20/21-031

INVITATION TO NEGOTIATE

THE STATE OF FLORIDA

DEPARTMENT OF MANAGEMENT SERVICES

Contents

1. Statement of Work

This statement of work addresses the planning, operational, and migration services that are provided by the State of Florida's Data Center to its customers. At the direction of Governor Ron DeSantis, the Department of Management Services (the Department) is leading efforts to deliver a more agile, cloud ready, and enterprise approach to technology. The Department currently provides data center services to state agencies pursuant to Section 282.201, F.S. The Department intends to outsource these data center services to a Contractor, who will operate the State Data Center (SDC), facilitate the state's migration to the cloud, enhance cybersecurity, and improve data interoperability. The intent of this procurement is to establish a multi-year Contract which meets the goals of the ITN as stated in section 1.4 of that document. Any contracted services will be available for use by State agencies and political subdivisions of the state, municipalities, and nonprofit corporations in accordance with Chapter 282, Florida Statutes (F.S.).

This Attachment A – Statement of Work (SOW) contains operational and administrative objectives for SDC that will form the requirements for implementation and on-going support under any Contract resulting from this ITN.

This SOW is intended to reflect the requested service components the Department is seeking the Respondent to offer for the SDC. This SOW includes references to service components that "must", "shall", or "will" be delivered. The Department intends for these SOW references to become mandatory at the time of Contract execution (as reflected in the Department's Request for Best and Final Offer). However, these SOW references may be subject to negotiation during the procurement and will be resolved through the terms of the Department's Request for Best and Final Offer.

While the Department reserves the right to negotiate any term or condition during the negotiation process, the Contractor agrees that its Reply is based on the assumption that the terms and conditions of the SOW (Attachment A), as well as the Draft Contract (Attachment B) of the ITN, apply as currently written.

1.1 Definitions

Claimant – A subject whose identity is to be verified using one or more authentication protocols (NIST 800-63-2).

Credential – An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber. While common usage often assumes that the subscriber maintains the credential, NIST Special Publication 800-63-3 also uses the term to refer to electronic records maintained by the Credential Service Provider (CSP) that establish binding between the subscriber's authenticator(s) and identity. (National Institute of Standards and Technology- NIST 800-63-3)

Customer – An entity that obtains services from the Department of Management Services. (Section 282.0041, F.S.)

Data – A subset of structured information in a format that allows such information to be electronically retrieved and transmitted. (Section 282.0041, F.S.).

Department – The Department of Management Services. (Section 282.0041, F.S.).

Enterprise – All Florida state agencies and the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services. (Section 282.0041, F.S.).

Enterprise architecture – A comprehensive operational framework that contemplates the needs and assets of the Enterprise to support interoperability. (Section 282.0041, F.S.).

Identity – The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity. (NIST 800-161)

Information technology – The equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form. (Section 282.0041, F.S.).

Interoperability – The technical ability to share and use data across and throughout the Enterprise. (Section 282.0041, F.S.).

Least Privilege – A security principle that restricts the access privileges of authorized personnel (e.g., program execution privileges, file modification privileges) to the minimum necessary to perform their jobs.

Open data – Data collected or created by a state agency, the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services, and structured in a way that enables the data to be fully discoverable and usable by the public. The term does not include data that are restricted from public disclosure distribution based on federal or state privacy, confidentiality, and security laws and regulations, including, but not limited to, those related to privacy, confidentiality, security, personal health, business or trade secret information, and exemptions from state public records laws; or data for which a state agency, the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services is statutorily authorized to assess a fee for its distribution. (Section 282.0041, F.S.).

Project – An endeavor that has a defined start and end point; is undertaken to create or modify a unique product, service, or result; and has specific objectives that, when attained, signify completion. (Section 282.0041, F.S.)

Separation of Duties – An internal control concept of having more than one person required to complete a critical process. This is an internal control intended to prevent fraud, abuse, and errors. (Chapter 60GG-2, F.A.C.)

Standards – Required practices, controls, components, or configurations established by an authority. (Section 282.0041, F.S.)

State agency – Means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. The term does not include the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services. (Section 282.0041, F.S.)

System Security Plan – Formal document that provides an overview of the security requirements for an information system and describes the security controls in place for meeting those requirements, as defined in NIST Publication 800-53 Rev.4.

Token – Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous editions of SP 800-63, this was referred to as a token. (NIST 800-63-3)

Transaction – A discrete event between a user and a system that supports a business or programmatic purpose. A government digital system may have multiple categories or types of transactions, which may require separate analysis within the overall digital identity risk assessment. (NIST 800-63-3)

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NIST 800-53 Rev.4)

1.1.1 Requirements Overview

This Statement of Work details the current state of operations, which includes existing service level agreements with customers, hardware and software inventories, and staff inventories in sections 1.1.1 through 1.2.1.15. In sections 1.3 through 1.6, additional requirements are detailed. The intent is for submissions to meet or exceed current service levels and meet the criterion in sections 1.1 through 1.6.

1.1.2 Background

Upon taking office, Governor Ron DeSantis took swift action and recommended immediate changes to the state's information technology policy. During the 2019 Legislative Session, the Administration successfully passed legislation to abolish the Agency for State Technology and move the remaining functions into the Department. Additionally, the bill changed the direction of the state's data storage strategy to focus on cloud computing solutions outside the footprint of the State Data Center (SDC). Additionally, the bill required state agencies to adopt a cloud first strategy in their procurements, required that agencies assess and report on the cloud readiness of their current applications that are operated in the SDC, and created a cybersecurity task force chaired by Lieutenant Governor Jeanette Nunez. The adopted cloud first policy requires that the SDC and state agencies show a preference for cloud computing solutions that minimize or do not require the purchasing, financing, or leasing of infrastructure at the SDC, that meet the needs of customer agencies, reduce costs, and meet or exceed applicable state and federal laws, regulations, and standards for information technology security.

Understanding that additional statutory changes would be required, the Administration successfully passed HB 1391 during the 2020 Legislative session which was subsequently signed into law by the Governor. The bill removed the telecommunications and public safety communications components of the "Division of State Technology" as a standalone Division and rebrands the remaining functions as the Florida Digital Service. With a focus on driving efficiencies through systems transformation and data interoperability, the bill requires the Department, through the Florida Digital Service, to establish Enterprise Architecture standards and assist state agencies with compliance to those established standards. Additionally, the bill requires FDS to create a comprehensive data catalog, as well as develop and publish a data dictionary and complete use cases to assist agencies in developing new technology solutions.

The SDC is located in the Capitol Circle Office Complex and is a Tier III facility. The SDC includes redundant power, backup generators, redundant network connections, disaster recovery services, colocation services and managed services for a variety of state agencies as well as other governmental agencies.

During fiscal year 2019-2020, the State of Florida contracted with a vendor for a business case to provide the Department with a formal recommendation for the best and most appropriate method for the Department to operate the SDC. That business case is included as an attachment to this Invitation to Negotiate (ITN) as Exhibit 1 - Business Case for State Data Center, Nonredacted. The business case recommends that the most effective method to manage the SDC is to leverage a contracted managed service provider to run data center operations, facilitate the state's migration to the cloud, enhance cybersecurity, and improve data interoperability.

The requirements are delineated by the current service offerings, service level agreements with customers, hardware and software asset inventory, and staff inventory. The State would like the Contractor to assume all current contracts and assets, where possible as determined during negotiations. Ownership of the SDC facility may be maintained by the State of Florida. Additionally, areas of required enhancement over current operational levels are detailed in the cloud first, interoperability, and cyber security sections. Contractor shall pay for its own utilities for the SDC facility. The State would like the Contractor to lease the SDC facility building from the State for the duration of the contract, as determined during negotiations.

1.1.3 Current State Data Center Services

The SDC is housed in a state-owned building that is 27,228 SF in size, 12,600 SF data center, plus areas for Mechanical, Electrical, Plumbing, and support areas. The data center space consists of 245 cabinets on a 32" raised floor. The Electrical service is rated at 880 KW of N+1 capacity with 459 KW currently in use. 8,256 SF in the data center is classified as high availability (Tier III Certified in 2008) with 182 Cabinets, 3 total UPS cabinets, two 1000 KW generators, and two 550 KW UPS units. The remaining 3,344 SF is classified as Fault Tolerant (Tier II and Uncertified) with 54 Fault Tolerant cabinets, 6 UPS cabinets, one 1000 KW generator, one 600 KW generator, and two 80 KW modular UPS units.

The current service offerings from the SDC are captured in the service catalog. The current 2020-2021 service catalog is included as Exhibit 2 - 2020-2021 Service Catalog. Please see the catalog for the detailed description of the service offerings. There are twelve categories of data center

services offered at the SDC listed below. All SDC services except for Direct Services are cost allocated amongst the customers who utilize the service. Direct Services are specialized services that a single customer receives from the SDC and costs for these services are allocated to the single customer that receives the service.

1. Backup and Recovery Services – These services include data protection services, data archival services, and data restoration services, offering multiple backup environment for compatibility as well as real time offsite data replication services. Specialize requirements are available as a direct service offering.
2. Cloud Services – These services include Enterprise Vault Cloud and Microsoft Azure Compute Cloud. Other cloud services, such as consulting, design, deployment and maintenance services are Direct Service offerings.
3. Database Services – The SDC provides Oracle, DB2 and Microsoft SQL database services to its customers with a range of availability, performance and application offerings for each database platform.
4. Data Center Facility and Operations Services – This constitutes the colocation services offering with a range of floor space, rack space, power and cooling offerings for SDC customers.
5. Mainframe Services – The SDC provides mainframe services to several agencies that operate significant applications on the mainframe platform which includes compute, storage, networking, and disaster recovery services.
6. Managed Applications – The SDC provides Citrix as a managed application to the SDC customer set. The SDC maintains the availability of the managed application including the hardware, operating system, storage, networking, disaster recovery and backup.
7. Network Services – The SDC provides standard networking services including network load balancing, proxy services, and monitoring services for network uptime.
8. Open Systems Services – The SDC provides services associated with Electronic Data Interchange, highly available web hosting and secure file transfer services, Linux/Unix compute services, and Linux/Unix managed server services to SDC customers.
9. Storage Services – The SDC provides both block-based and object-based storage services to the customers of the SDC. The SDC also provides media disposal services as a Direct Service to the SDC customers.
10. Windows Services – The SDC provides Microsoft Windows capacity units and Windows managed server services to the SDC customers.
11. Direct Service Offerings – Besides the Direct Services offerings defined above, the SDC provides Security Training services and IT consulting services across a broad range of technologies.
12. Cloud-Based Custom Support Offerings – The SDC provides Application Readiness Assessment for the Cloud, Design and Architectural reviews, Cloud Transition and

Migration services, Routing and Traffic Management services and Firewall Management services.

1.1.4 Current State Data Center Service Level Agreements

The current service level agreements with the SDC are captured in Exhibit 3 - Service Level Agreement (SLA).

1.1.5 Current Asset Inventory

1.1.5.1. Hardware

The SDC currently owns, leases, and finances hardware platforms that are in production use. The list of current hardware is included as Exhibit 4 - Hardware. The Department intends to assign ownership of hardware, remaining financing payments for financed hardware, and leases for hardware to the Contractor. The Department will discuss the process for assigning hardware under the Contract with Respondents during negotiations.

1.1.5.2. Software

The SDC owns perpetual software licensing as well as subscription-based software products. The list of current software is included as Exhibit 5 - Software. The Department intends to assign ownership of perpetual software licensing and any subscriptions required to maintain service to the Contractor. The Department will discuss the process for assigning software licensing under the Contract with Respondents during negotiations.

1.1.6 Current Staffing Inventory

The SDC is currently staffed with State of Florida employees and contracted staff augmentation personnel. The salaries and benefits information for those State of Florida employees are included in Exhibit 6 - State Employee Inventory. The staff augmentation contractors and their rates are included in Exhibit 7 - Contracted Staff Inventory.

1.2 Staffing

1.2.1 The Contractor shall provide sufficient, qualified personnel to oversee and carry out the services required by this Contract as delineated in section 1.2.1.14. Contractor shall designate individuals within its organization to be contacts for the Department and its Customers in accordance with the following subsections:

1.2.1.1 The Contractor staffing responsibilities include conducting all components of the Contract in a timely, efficient, productive, consistent, courteous and professional manner.

1.2.1.2 The Contractor shall devote the staffing time and resources necessary to successfully manage the Contract and provide the services, including having sufficient staff available for telephonic, email and on-site consultations.

1.2.1.3 The Contractor shall provide each of its staff members orientation and training on all components of the Contract prior to working on any component of the Contract. Contractor shall provide the Department's Contract Manager with documentation of this training upon request.

1.2.1.4 The Contractor is required to employ all key staff positions as described in this SOW as delineated in section 1.2.1.15.

1.2.1.5 It is understood and agreed that from time to time a vacancy may occur in key staff positions. For purposes of this Contract, a vacancy occurs when: the position is not initially filled; the position is not filled due to a resignation, retirement, termination, or reassignment, or; the position is filled with a person who does not possess the minimum qualifications required to perform the job duties. A vacancy does not occur when an employee is temporarily absent due to vacation, sick leave, or other temporary leave condition such as training. In the case of a vacancy, the Contractor may arrange for the job duties to be provided by another employee who meets the minimum job qualifications until this position is filled.

1.2.1.6 The Contractor will fill vacancies of key staff positions within sixty (60) calendar days of vacancy.

1.2.1.7 The Contractor may request a waiver from the Department's Contract Manager if it believes it has good cause to not fill a key staff position within the required timeframe. The Department will review any such requests on a case-by-case basis and respond within a reasonable timeframe. Determination of all waiver requests are at the sole discretion of the Department.

1.2.1.8 The Contractor shall notify the Department of all vacancies of key staff positions.

1.2.1.9 The Contractor will only fill key staff positions with persons that fulfill the minimum job qualifications in accordance with 1.2.1.15 of this SOW.

1.2.1.10 The Department reserves the right to review and approve candidates being considered by the Contractor for a key staff position described in this Contract which will suspend the SLA clock during the Department review.

1.2.1.11 The Department will have the right to require the replacement of any staff who serve in a key staff position or as part of the Customer Service Team, and Contractor will remove such staff within ninety (90) calendar days' or earlier upon the Department's notice to Contractor.

1.2.1.12 The Contractor must provide a sufficient number of Contractor staff to handle the workload projected for the start of the Contract and shall be scalable and flexible, so staffing can be adapted as needed.

1.2.1.13 The Contractor will develop and provide to the Department for approval a Staffing Organizational Chart to be implemented throughout the Contract and this Staffing Organizational Chart will be reviewed annually with the Department.

1.2.1.14 The Contractor is required to provide sufficient, competent and capable staff to provide complete and timely services as required by the Contract. In the event the Department

determines the Contractor has a staff deficiency, it will notify the Contractor in writing. A staff deficiency will include, at the Department's discretion, insufficient number of staff, or insufficient level of competency in staff, to provide complete and timely services under this Contract. A staffing deficiency will also include the retention of staff thirty (30) days past a Department Contract Manager's requirement to remove that staff member. The Contractor must remedy the identified staffing deficiencies by adding or replacing staff as required by the Department.

1.2.1.15 Key positions and requirements include:

A. Data Center Director

Minimum Required Skills and Required Qualifications	**Minimum Years of Experience**
Experience leading IT Project teams	10
Operational Infrastructure Management	10
Technical understanding of cloud computing, virtualization, storage area networks, backup and data production, disaster recovery, database services, local & wide area networks, servers, mainframe, IT security, IT asset management, IT service management, and data center operations.	10
IT operational planning and process design	7
Configuration management and change control	5
Business case development	5
Personnel Management	7
Technical and Strategic Planning	5
Knowledge of cloud technologies and migration strategies	3

B. Infrastructure Manager

Minimum Required Skills and Required Qualifications	**Minimum Years of Experience**
Project evaluation and feasibility assessment	7

Workflow analysis and work scheduling	5
Experience participating in IT Project teams	5
Knowledge of security principles, network, storage, backup and disaster recovery technologies and systems.	7
Security risk mitigation	5
Knowledge of data center technologies and requirements of a shared data center environment.	5
Technical and Strategic Planning	5
Expertise in the architecture and design of IT infrastructure solutions	5
Experience in maintaining, securing, and controlling the application of upgrades, service packs, patches, firmware, configuration backups, and maintenance agreements of systems	5
Knowledge of corresponding cloud technologies and migration strategies	3
Expertise in virtualization technologies	5

C. Database Manager

Minimum Required Skills and Required Qualifications	**Minimum Years of Experience**
Project evaluation and feasibility assessment	5
Workflow analysis and work scheduling	5
Experience participating in IT Project teams	5
Knowledge of security principles and security risk mitigation	5
Knowledge of system (Oracle, UDB, DB2, MS-SQL etc.)	5
Knowledge of data center technologies and requirements of a shared data center environment.	5
Technical and Strategic Planning	5

Knowledge of database products and licensing requirements	7
Expertise in the architecture and design of database solutions including backup, recovery, and disaster recovery solutions	5
Experience in maintaining, performance tuning, securing, and controlling the application of upgrades, service packs, patches, firmware, configuration backups, and maintenance agreements of systems	5
Knowledge of corresponding cloud technologies and migration strategies	3

D. Server Manager

Minimum Required Skills and Required Qualifications	**Minimum Years of Experience**
Project evaluation and feasibility assessment	5
Workflow analysis and work scheduling	5
Experience participating IT Project teams	5
Knowledge of security principles and security risk mitigation	5
Knowledge of system (Linux/Unix, Windows, etc.)	5
Knowledge of data center technologies and requirements of a shared data center environment.	5
Technical and Strategic Planning	5
Expertise in the architecture and design of server solutions	7
Experience in maintaining, securing, and controlling the application of upgrades, service packs, patches, firmware, configuration backups, and maintenance agreements of systems	5
Experience maintaining inventories of systems and capacity	3
Knowledge of corresponding cloud technologies and migration strategies	3

Expertise in virtualization technologies	5

E. Information Security Manager

Minimum Required Skills and Required Qualifications	**Minimum Years of Experience**
Customer service experience	5
Project evaluation and feasibility assessment	5
Experience participating in IT project teams	5
Experienced in evaluating, recommending, and implementing systems for detection and prevention of information privacy and security breaches.	5
Skilled in evaluating systems for compliance with information privacy and security policies and procedures, federal and state laws, and industry standards through a risk assessment process.	5
Expertise in the architecture and design of information security solutions	5
Experience in maintaining, securing, and controlling the application of upgrades, service packs, patches, firmware, configuration backups, and maintenance agreements of systems	5
Knowledge of corresponding cloud technologies and migration strategies	3
Experience leading in CSIRT (Cyber Security Incident Response Teams)	3
Experience with IDS/IPS, threat detection, log aggregation, threat hunting, and endpoint protection	5

F. Customer Service Manager

Minimum Required Skills and Required Qualifications	Minimum Years of Experience
Customer service experience	5
Project evaluation and feasibility assessment	3
Experience coordinating activities between SDC and customers	3
Experience participating in IT Projects	3
Ability to solve complex problems	3
Conflict resolution skills	3

G. Facilities Manager

Minimum Required Skills and Required Qualifications	Minimum Years of Experience
Leading IT project teams and work scheduling	7
Operational Infrastructure Management	7
Data center operations and facilities management	10
IT operational planning and process design	7
Data center solution architectural design	5
Business case development	5
Personnel Management	7
Technical and Strategic Planning	5
Experience maintaining inventories systems and capacity	5
Experience implementing new systems and changes	7
Expertise in the coordination of maintaining, securing, and controlling the application of upgrades, service packs, patches,	7

firmware, configuration backups, and maintenance agreements of systems	
Experience overseeing data center facilities and infrastructure	7

H. Cloud Migration Manager

Minimum Required Skills and Required Qualifications	**Minimum Years of Experience**
Project evaluation and feasibility assessment	5
Workflow analysis and work scheduling	5
Experience participating in IT project teams	5
Knowledge of security principles and security risk mitigation	5
Ability to consult with customers on developing cloud migration strategies	3
Technical and Strategic Planning	5
Expertise in the coordination of maintaining, securing, and controlling the application of upgrades, service packs, patches, backups, and maintenance agreements of systems	5
Experience with Cloud design, configuration, implementation, and support, including Cloud migrations from on-premise technologies including SaaS, PaaS, IaaS, and serverless technologies	5

I. Interoperability Manager

Minimum Required Skills and Required Qualifications	**Minimum Years of Experience**
Project evaluation and feasibility assessment	5
Workflow analysis and work scheduling	5
IT Project Management and scheduling	5
Knowledge of enterprise data architecture	5

Ability to consult with customers on interoperability of data and enterprise architecture	3
Technical and Strategic Planning	5
Experience implementing data system integrations	5

J. Account Executive

Minimum Required Skills and Required Qualifications	**Minimum Years of Experience**
Experience managing large data center or other IT customers	7
Skilled customer service provider	10
Ability to solve complex problems	7
Authority to make decisions on behalf of the Contractor	N/A
Experienced with IT Projects	5
Skilled at conflict resolution	7
Experience working with government customers (federal, state, and or local customers)	5

All key positions are required to have the following knowledge, skills and abilities:

- Expert written and verbal communication skills, and meeting facilitation experience
- Expert customer service skills
- Conflict resolution experience
- Research and analysis skills
- The ability to participate in Continuity of Operations and Disaster Recovery planning and trial exercises
- Leadership and managerial experience
- Ability to adhere to Service Level Agreements
- Advanced knowledge of Florida statutes, administrative code, and Department policies governing the SDC and technology in the State of Florida
- Maintain current knowledge of industry trends, advances in technology, and security threats
- Bachelor’s degree in technology, business, or related field, or equal experience in lieu of education.
- Provide resume and certifications to confirm skills and experience meet the minimum requirements for key positions.

1.3 Start of Contract Transition Services

1.3.1 The Contractor will be required to submit a transition plan for resources, personnel and services within sixty (60) days of execution of the Contract with sufficient detail for the Department's review and approval. The Department reserves the right to request modifications.

1.3.2 The Contractor and the Department will establish dates and times for transition phases.

1.3.3 The Contractor will provide details regarding when interviews of SDC personnel will be conducted.

1.3.4 The Contractor will retain transitioned SDC employees for at least 1 year.

1.3.5 Transition Project Management

Vendor shall appoint a PMP certified Project Manager to lead the transition of the State Data Center to the Master Services Provider (MSP). The selected MSP will follow project management requirements set forth in Chapter 60GG-1, F.A.C. (Project Management and Oversight). The MSP will participate in the identification, analysis, and mitigation of risks and issues. The MSP Project Manager (and other team members as required) will coordinate all activities with the DMS assigned Project Manager.

The MSP will provide weekly status reports to the Department of Management Services and its IV&V vendor during transition. The status reports will include all information stated in Chapter 60GG-1, F.A.C. (Project Status Report). The project schedule will be provided in MS Project format on a weekly basis, and the schedule must be developed to meet scheduling best practices.

1.4 Cloud First

Section 282.206, F.S., requires that each state agency adopt a cloud first strategy in procurements and a strategic plan, updated annually, that identifies and documents the readiness, appropriate strategy, and high level timeline for transition to a cloud-computing service based on the application's quality, cost, and resource requirements.

The Department has also promulgated rules within Chapter 60GG-4, F.A.C., which governs cloud computing. The rule requires agencies to consult with the Department prior to the procurement of cloud services to ensure compatibility and security pursuant to Chapter 60GG-2, F.A.C., On or before October 15th of each year, each agency will provide to the Department a list of applications and workloads that have been migrated to the cloud. Each agency will ensure that security and interoperability with applications that interface outside the cloud service provider's cloud are well documented.

Agencies will also consult with the Department prior to the use of cloud-based services where the Department's allocated IP addresses will be assigned to cloud-based resources that have SDC or state intranet connectivity requirements and will document this consultation in writing.

1.4.1 Support for Customer Cloud First Procurement Strategy Development

A. The Contractor will provide support to SDC customers and the Department in the development of each customer's cloud first procurement strategies, including best practices and policy development.

B. The Contractor will develop a sample policy and procedure.

C. The Contractor will provide templates for cloud procurement policies incorporating best practices to assist the agency in complying with Chapter 60GG-4, F.A.C.

1.4.2 Support for Customer Application Cloud Migration Plan Development

A. The Contractor will provide support to SDC customers and the Department as they complete their evaluations of the cloud readiness of their application inventory.

B. The Contractor will develop templates for the evaluation of application readiness, appropriate strategies, and timelines for transition of application types to a cloud service provider.

C. The Contractor will develop templates for reporting the inventory of SDC customer applications as to their readiness, appropriate migration strategies, and high-level timelines for transition of the agency's applications to the cloud.

1.4.3 Support for Execution of a Customer Application Cloud Migration Plan

A. The Contractor will provide support to SDC customers and the Department in the execution of each customers cloud migration plan for each application identified by SDC customers that will migrate to a cloud service provider.

B. The Contractor will provide templates which will serve as checklists for the steps to migrate an SDC customer's application to a specific cloud service provider based on the selected migration strategy, the chosen service model, the chosen deployment model, and the data classification pursuant to Chapter 60GG-2, F.A.C.

1.4.4 Support for Customer Development of Cloud Service Level Agreements

A. The Contractor will provide support to SDC customers and the Department in the development of cloud service level agreements (SLA) which provide requirements for availability, performance, and application response.

B. The Contractor will develop SLA templates for cloud applications which SDC customers can use to develop application specific service level agreement terms for their cloud computing contracts.

1.5 Enterprise Architecture

Section 282.0051, F.S., requires the Department to recommend potential methods and opportunities for standardizing data across state agencies to promote interoperability and reduce the collection of duplicative data. Furthermore, the Department shall recommend open data

technical standards for use by each state agency. The Contractor will comply with Section 282.0051, F.S., and Chapter 60GG-5, F.A.C.

The State of Florida has prioritized solutions to further data sharing and integration since the passage of House Bill 5301 in 2019 and with the passage of House Bill 1391 in 2020. The Department must develop an Enterprise Architecture which acknowledges the unique needs of each entity within the Enterprise in the publication of standards and terminologies to facilitate digital interoperability.

The Department must create and maintain an enterprise data catalog which provides a comprehensive listing of data elements and the legacy systems or applications in which the elements are located. The Department must also identify all data restricted from public disclosure and provide a data dictionary for each agency.

Agencies will be required to notify the Department prior to any planned procurement of an Information Technology project that is subject to enterprise architecture standards and participate with the Department to develop specifications or recommend modifications to procurements to ensure compliance with enterprise architecture standards, or provide a justification for adopting alternative standards that explains how data interoperability will be achieved pursuant to Section 282.00515, F.S.

1.5.1 Support for Customer Enterprise Architecture Procurement Strategy Development

A. The Contractor will provide support to SDC customers and the Department in the development of each customer's procurement strategies, including best practices and policy development, to ensure compliance with enterprise architecture standards and interoperability with existing systems.

B. The Contractor will provide templates and procedures to support SDC customers in the development of each customer's procurement objectives, to ensure compliance with enterprise architecture standards and interoperability with existing systems.

C. The Contractor will provide templates and procedures to facilitate SDC customer alternatives to the enterprise architecture standards.

1.5.2 Support for Infrastructure Modernization to Promote Interoperability

A. The Contractor will provide support to SDC customers and the Department in the development of each customer's architecture strategies, including best practices and policy development, to ensure compliance with enterprise architecture standards, promote cost savings by avoiding duplicative efforts, and ensure new IT systems can interoperate across the enterprise.

B. The Contractor will identify and deploy technology, which complies with the enterprise architecture standards, to securely modernize the SDC's offerings to allow interoperability and data sharing between agencies in order to reduce costs.

1.5.3 Support for Customer Enterprise Data Catalog

A. The Contractor will provide support to SDC customers and the Department in the development of each customer's data strategy, including best practices and policy development, to ensure integration with the enterprise data catalog and security of confidential data.

B. The Contractor will develop templates for reporting the changes to SDC customer applications and data architecture to ensure those changes can be reflected in the enterprise data catalog.

1.6 Cyber Security

The Contractor shall ensure that the SDC's cybersecurity complies with Section 282.318, F.S., and Chapter 60GG-2, F.A.C., Florida Cybersecurity Standards (FCS).

The Contractor shall abide by all federal law, state statute, and other prescribed security guidance, to include (but not limited to) those requirements outlined for such sensitive data types as Personally Identifiable Information (PII), Protected Health Information (PHI), and Criminal Justice Information (CJI).

The Contractor must ensure that their security monitoring environment integrates with the SDC's current security and host logging capabilities during transition to ensure that it receives accurate and timely logs.

1.6.1 Security Policy and Documentation

A. The Contractor will maintain security documentation for the SDC.

B. The Contractor will review and update the security documentation quarterly.

C. The Contractor will provide expert analysis of changes to the SDC's security environment to SDC customers.

D. The Contractor will track and analyze new state legislative security initiatives, NIST policy changes, Departmental rulemaking, agency and customer requirements. Based on the analysis and anticipated impacts, the Contractor will develop security recommendations tailored to SDC customer needs.

1.6.2 System Security Plan Requirements

A. The Contractor will develop and provide to the Department a system security plan for the SDC, security plans for managed information systems, and any associated plans of action developed to satisfy the security requirements of Chapter 60GG-2, F.A.C., and in accordance with NIST Special Publication (SP) 800-171 to describe the Contractor's information system infrastructure comprising the SDC.

B. The Contractor will include proposed changes to the system security plan to reflect any infrastructure changes or new service offerings within the SDC prior to approval of those changes by the Department.

C. The Contractor will review the system security plan with the Department and update the security plan quarterly.

1.6.3 Security Assessment and Control Implementation

A. The Contractor shall complete and submit a comprehensive security risk assessment to the Department as defined by Section 282.318(4)(d), F.S., and Rule 60GG-2.002(4)(a), F.A.C. This initial assessment shall be provided in a Department specified format within 90 days of the contract start date and additionally include a Plan of Action and Milestones (POA&M) for remediation of findings. Future comprehensive security risk assessments shall be completed no later than July 31, 2023, and every three years thereafter. The security risk assessment will align with the current Cyber Security Framework (CSF), NIST. The department may conduct a security risk assessment using an independent third-party.

B. The Contractor will establish log retention schedules with each SDC customer based on statutory requirements, resource availability, and criticality of the logs.

C. The Contractor will collect, maintain and secure required log records, in accordance with customer-developed retention schedule. The Contractor shall make all logs available to the customer through direct API or other acceptable method.

D. The Contractor will conduct site audits, pursuant to Chapter 60GG-2, F.A.C., of the information technology and information security controls for all facilities used in complying with its obligations under the contract, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on recognized industry best practices.

E. The Contractor will develop a control implementation summary document that defines security control responsibilities for each information system in the SDC for the Contractor, the SDC customer, and the Department, pursuant to Chapter 60GG-2, F.A.C.

F. The Contractor will provide recommendations and guidance for corrective action of all non-compliant security controls.

G. The Contractor will provide security expertise to ensure security controls are implemented and will maintain the resulting documentation and security artifacts as current.

H. The Contractor will implement and maintain customer defined security metrics, pursuant to Chapter 60GG-2, F.A.C.

1.6.4 Access Control and Identity

A. The Contractor will ensure that access to IT resources is limited to authorized users, processes, or devices, and to authorized activities and transactions, pursuant to Chapter 60GG-2, F.A.C.

B. The Contractor will manage identities and credentials for authorized devices and users and ensure control measures shall, at a minimum, include authentication token(s) unique to the individual.

C. The Contractor will manage access permissions by incorporating the principles of "least privilege" and "separation of duties."

1.6.5 SDC Endpoint Security Management

A. The Contractor shall monitor and manage SDC Customer endpoint resources, including, but not limited to, servers, virtual desktop infrastructure, and network devices for evidence of threats, indicators of compromise, and malware, providing alerts when an endpoint resource may be compromised or malware is detected.

B. The Contractor shall develop templates for reporting the changes to SDC customer applications and data architecture to ensure those changes can be reflected in the enterprise data catalog.

C. The Contractor shall provide an Endpoint Management solution that will automate detection and provide policy actions to bring devices into compliance.

D. The Contractor shall install, operate, and maintain Malware protection software and systems in accordance with SDC Customer security requirements for Software and Equipment in the Customer Environment as per agreement with the Customer.

E. The Contractor shall provide a Centralized Security Data Repository which contains all relevant information regarding scan results including scan date, systems scanned, software used in the scan, and any affected systems if malware is detected.

F. The Contractor shall, upon detection of a malware infection, immediately, as defined by the applicable Security Incident Severity Level, notify the SDC customer and the Department and respond to malware infections as directed by SDC Customer policy.

G. The Contractor shall respond to a malware infection and determine if any data was leaked, share malware binaries and malicious URLs with the SDC customer, and track malware incidents within the Security Repository.

H. The Contractor shall eradicate Malware through standard security response techniques on SDC customer Endpoint systems.

1.6.6 Continuous Monitoring Program

A. The Contractor will design, develop, and implement, in compliance with Chapter 60GG-2, F.A.C., a continuous monitoring process across all major SDC information systems, as defined in NIST Special Public 800-137, to provide assurance at least quarterly to the Department on the security protections of major information systems.

B. The Contractor shall provide Network Security Monitoring, Alerting and Analysis Services that monitors the SDC networks for external intrusions and cyberattacks and notifies the proper State authorities so that countermeasures may be taken.
C. The Contractor will ensure that electronic audit records allow actions of users to be uniquely traced to those users. These records must describe collected data points and correlation analysis parameters.
D. Contractor shall provide highly-available Security Information and Event Management (SIEM) services that provides real-time analysis of security alerts generated by SDC customer applications and systems and provide access to that analysis to the Department and SDC customers. Contractor may provide SIEM services for applications that have been migrated to the cloud by SDC customers, as determined during negotiations.
E. The Contractor shall provide a secure encrypted channel to receive SIEM log data into a central security repository.
F. The Contractor shall provide log management and analysis monitoring which provides automated alert response mechanisms with corresponding actions for resolution to the Department and SDC customers, supports unique identification of individuals, permits an audit of the logs to trace activities through the system, including the capability to determine the exact confidential or exempt data accessed or transmitted by the individual, converts different log formats into a common format, and stores data for a minimum of 30 days or according to SDC customer retention requirements.

1.6.7 Security Incident Reporting and Response

A. The Contractor shall provide the SDC customers and Department with the name and contact information of a Contractor employee who shall serve as the primary security contact for the SDC customer or the Department who shall be available to assist Customer or the Department twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a security incident, as defined in Section 282.0041, F.S.

B. The Contractor will notify an SDC customer and the Department Information Security Manager (ISM) of a Security Incident as soon as practical, but no later than four (4) hours after Contractor becomes aware of the Security Breach.

C. The Contractor will ensure the security incident reporting process includes notification procedures, established pursuant to Section 501.171 and 282.318, F.S., and as specified in executed agreements with external parties.

D. The Contractor will assist SDC customers and the Department with reporting incidents to the Department and the Cybercrime Office (as established within the Florida Department of Law Enforcement via Section 943.0415, F.S.) and will provide detailed information related to indicators of compromise, pursuant to Chapter 60GG-2, F.A.C., to the Department ISM and to the Cybercrime Office to provide early warning and proactive response capability to other State of Florida agencies.

E. The Contractor shall coordinate with the Department ISM and the SDC Customer, immediately following Contractor's notification of a security incident, to investigate the security incident.

F. The Contractor agrees to fully cooperate with the SDC Customer in Customer's handling of the matter, including, without limitation:

1) Assisting with any investigation.

2) Providing Customer with physical access to the facilities and operations affected.

3) Facilitating interviews with Contractor's employees and others involved in the matter.

4) Making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise reasonably required by Customer.

G. The Contractor shall establish a Computer Security Incident Response Team (CSIRT) to respond to cybersecurity incidents. The SDC Customer's ISM for those customer's systems impacted by the incident and the Department's ISM (or designee) will be members of this CSIRT team for the duration of the response to the security incident.

H. The Contractor shall take reasonable steps, at the Contractor's expense, to immediately remedy any Security Breach and prevent any further Security Breach in accordance with applicable privacy rights, laws, regulations and standards.

I. The Contractor agrees that it shall not inform any third party, excluding the Department, of any Security Breach without first obtaining Customer's prior written consent, other than to inform a complainant that the matter has been forwarded to Customer's legal counsel.

J. The Contractor agrees that Customer shall have the sole right to determine:

1) Whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Customer's discretion.

2) The contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

1.6.8 Threat Research

A. The Contractor shall provide support to SDC customers and the Department in the area of threat research and identification.

B. The Contractor shall develop plans to correlate information targeted to an SDC Customer's environment with knowledge of extant threats to assist in structuring pro-active response to credible threats. This service is in addition to any threat research required to perform other Services in this statement of work.

C. The Contractor shall collect intelligence and formulate action plans to implement mitigation strategies based on identified threats, develop a profile of extant threats

targeted to the SDC and Customer environments, identify potential resources, tools, and techniques that could be used to prevent the exploitation of the identified threats, catalog credible threats to which the SDC customers may be vulnerable.

D. The Contractor shall identify compromise of authentication credentials, provide analysis of enterprise trends and significant security events that impact SDC customers, prioritize vulnerability management activities based on risk criteria that include the likelihood of a given threat materializing.

E. Contribute to an enterprise-managed Threat Intelligence Platform (TIP) through the submission of indicators of compromise (IOCs) relevant to the defense of SDC customer networks.

2. Deliverables

2.1 Staffing Plan

This section is applicable to all services. The terms “Contractor staff” and “staff” include all staff employed by the Contractor and by its subcontractors providing services under the Contract.

2.1.1 Staffing Plan Requirements

2.1.1.1 The Staffing Organizational Chart will include all staff resources assigned to all components of the Contract to be approved by the Department. The final Staffing Organizational Chart must contain names, titles, and number of staff (full-time and part-time) proposed to support the Contract. The Contractor’s final Staffing Organizational Chart shall include a justification for the number of staff and the percentage of time each staff person will devote to the Contract.

2.1.1.2 Resumes and relevant certifications for proposed Key Personnel to confirm required skills and experience will be provided.

2.2 Start of Contract Transition Plan

2.2.1. The transition plan shall be comprised of the following components:

A. Detailed schedule for transition of services within the SDC.

B. The potential SDC customer impacts (e.g., business needs, complexity of service, services impacted by special programs, Federal recertification processes, etc.).

C. How the transition will be accomplished in the least disruptive way.

D. Identification of tasks dependent upon the State’s data or resources.

E. The project management plan for transition as defined below.

2.2.2. The Contractor will provide detailed project documentation, in compliance with Chapter 60GG-1, F.A.C., for the transition component of the contract which will include:

A. Project Charter

B. Project Deliverables

C. Project Schedule with start dates, end dates, tasks, dependencies, and critical path.

D. Work Breakdown Structures

E. Resource Plans including State resources needed for transition support

F. Risk Register and risk mitigation strategies.

G. Maintain action item logs, issue logs, and decision logs

H. Budget

I. Communication Plan

J. Stakeholder List

K. Weekly Status Reports to include project status, variance, risks and issues, changes, milestones, deliverables, and major tasks.

L. Requirements traceability matrix

M. Project Management Plan to include:

1) Resource management plan

2) Schedule management plan

3) Communication management plan

4) Change management plan

5) Quality management plan

6) Risk and issue management plans

7) Deliverable acceptance plan

8) Cost management plan

2.2.3. The Contractor will provide a detailed Resource transition plan that will consist of:

A. List of SDC employees and contractors to interview

B. List of additional resources from the Contractor that will perform services under the contract.

C. Information concerning when interviews will be conducted for SDC personnel

2.2.4. The Contractor will offer one (1) year contracts to SDC employees who will be retained unless the contractor requests a waiver to the one (1) year retention requirement. The final decision on a waiver request will lie with the Department.

2.3 Cloud Migration Support Plan

The cloud migration support plan shall include the following components:

2.3.1 Cloud First Procurement Sample Policies

A. Sample policies and procedures for SDC customers to use as reference to establish their policies for a preference for cloud computing in procurements relating to SDC customer applications and systems at the SDC.

B. Templates which contain best practices for cloud computing procurement including sample evaluation criteria, scoring models and SLA terms and conditions for cloud solutions.

2.3.2 Application Cloud Readiness Evaluation and Reporting

A. Procedures which provide a step by step evaluation of an application's cloud readiness, a step by step process to select an appropriate cloud migration strategy, and a step by step process to develop a high-level timeline for cloud migration based on industry best practices.

B. Templates which list the factors to consider in determining an application's cloud readiness, the factors used to determine the best migration strategy for an application to a cloud provider and factors which will assist with the development of the high-level timeline.

2.3.3 Application Cloud Migration Execution

Sample cloud migration project management plans which consider the recommended migration strategy, likely resources required to complete the migration, sample work breakdown structures, sample timelines with key milestones and associated with the selected migration strategy.

2.4 Enterprise Architecture Support Plan

The interoperability support plan shall define how the Contractor will provide support for solutions to comply with all interoperability requirements and goals of the Department's Enterprise Architecture Standards, once adopted.

2.4.1. Enterprise Architecture Procurement Policy

A. Sample policies and procedures to properly ensure procurements for information technology projects comply with enterprise architecture standards and interoperability with existing systems.

B. Sample templates which contain best practices to properly ensure procurements comply with enterprise architecture standards, and allowances for exceptions to standards.

2.4.2. Infrastructure and Service Evaluation for Modernization and Interoperability

Sample templates which contain best practices to ensure infrastructure or service adoption and/or changes provide a cost savings by reducing duplicative efforts by SDC customers, improve interoperability and promote the use of shared resources.

2.5 Cyber Security Plan

The cyber security plan shall outline the information security methods, tools and procedures to provide compliance with Chapter 60GG-2, F.A.C., for systems and applications operated by SDC customers.

2.5.1. Security Policy and Documentation

A. Sample policies and procedures to properly ensure security for information technology systems at the SDC comply with Chapter 60GG-2, F.A.C.

B. Written analysis of changes to the SDC security environment, legislative initiatives, changes in NIST, agency or customer requirements.

2.5.2. SDC System Security Plan

Security plan for the SDC, security plans for managed information systems and any associated plans of action to ensure security for information technology systems at the SDC comply with Chapter 60GG-2, F.A.C.

2.5.3. Security Assessment and Controls

A. A comprehensive risk assessment as required by Section 282.318(4)(d), F.S.

B. A log retention schedule for each SDC customer.

C. An API or other access method for SDC customer access to logs maintained by the Contractor.

D. Audit reports for conducted site audits.

E. A control implementation summary document which defines security control responsibility for each information system at the SDC.

F. Written recommendations for corrective action of all non-compliant security controls.

2.5.4. SDC Endpoint Security Management

A. Reports of changes to SDC customer applications and data architecture.

B. A centralized security data repository containing security scan information.

2.5.5. Continuous Monitoring

A. Audit access records which uniquely trace actions in a system to a user.

B. Automated security alerts from the SIEM service operated by the Contractor.

2.5.6. Security Incident Reporting and Response

A. Cybersecurity Incident Response Plan with the following elements:
    1) Name of the security officer of the Contractor.
    2) Roles of individual positions during incident response.
    3) Specific stakeholder notification requirements.
    4) Annual training requirements specific to incident response.
B. Security Incident and Breach notifications.
C. Logs, data reporting and other materials for incident investigation.
D. Quarterly Security Incident Review meeting minutes.

2.5.7. Threat Research

A. Plans to correlate information threats targeted to an SDC customer.
B. Written analysis of security trends and significant security events.
C. Action plans for threat mitigation strategies.

2.6 Reports

The Contractor is required to provide the following reports on a recurring basis throughout the term of the Contract, as required by the Department. The Department will specify the content and format of the required reports, and the Contractor shall provide reports that meet the Department's requirements. The Contractor shall not make any content or formatting changes to required reports without receiving advance, written approval from the Department's Contract Manager.

1. Staffing Inventory reports
2. SLA performance reports
3. Security incident reports
4. Project Management reports during transition
5. Service offering cost analysis

As needed, the Department reserves the right to require additional reporting during the term of the Contract.

THIS SPACE IS INTENTIONALLY LEFT BLANK.

3 Performance Measures

3.1 Cyber security Performance Measures

Deliverable	Title	Specific Measure
2.6.1	Endpoint Resource Management	Based on vulnerability scans, identify Category 4 and 5 vulnerabilities and mitigate 100% of same within 30 days.
2.6.1	Endpoint Resource Management	Ensure that endpoint protection software deployed and functioning on newly provisioned devices within 1 hour of deployment.
2.6.2	Security Information and Event Management	Maintain a 99% availability of the Service Provider's SIEM instance
2.6.2	Security Information and Event Management	Capture and store network flow data at a fidelity of 1:100 for SIEM analysis.
2.6.3	Targeted Threat Research	Maintain at least .75% FTE within Security Operations Management devoted to targeted threat research.
2.6.3	Targeted Threat Research	Report high severity alerting received from external sources to customers within 1 hour.
2.6.4	Security Monitoring and Alerting Services	Incrementally decrease false positive rate of alerting to 3%, through improvement of a minimum of 2% per month.
2.6.4	Security Monitoring and Alerting Services	Incrementally improve verifiable true positive rate to 95%, through improvement of a minimum of 2% per month.
2.6.4	Security Monitoring and Alerting Services	Provide Customers with, at a minimum, two Proof-of-Concepts annually to evaluate new and emerging technologies.

3.2 Other Performance Measures

Current performance measures are included in Exhibit 3 – Service Level Agreements. Additional performance measures may be identified during negotiations.

4 Financial Consequences for Nonperformance

Subsection 287.058(1)(h), F.S., requires that the final contract negotiated by the Department contain financial consequences to be applied if the contractor fails to perform in accordance with the contract. Financial consequences will be negotiated between the Department and Respondent(s) during negotiations. The negotiated financial consequences will be incorporated into the final Statement of Work of the Contract that results from this ITN.

5 Additions/Deletions

During the term of the Contract, the need may arise for the Department to add or remove services that are being provided under the Contract, due to budgetary, legislative, technology or business requirement changes. During ITN negotiations, the Department intends to discuss the process for adding and deleting services and how costs for such additions and deletion will be determined by the Department and Contractor.

6 Quarterly Business Review Meetings

In order to maintain the partnership between the Department and Contractor, the Department may require a business review meeting each quarter. The Department may require specific attendees associated with Contractor's services provided under this Contract, either in person or by conference call. The business review meeting may include, but is not limited to, the following:

- Successful completion of deliverables;
- Review of Contractor's performance;
- Review of minimum required reports;
- Staffing support, changes and issues;
- Addressing any elevated Customer issues; and
- Review of continuous improvement ideas that may help lower total costs and/or improve business efficiencies.

During the term of the Contract, the Department reserves the right to require additional meetings, on a one-time or recurring basis, if deemed necessary. The Department will strive to provide the Contractor and its staff with advance notice of any such meetings and with reasonable accommodation of staff schedules.

7 End of Contract Transition Plan

The Contractor shall provide a transition plan to be executed upon written notice by the Department of its intent to commence the end of contract transition plan. This plan will operate on an eighteen (18) month timetable with no loss of service to the SDC customers. This plan will include, at a minimum, key milestones with identified responsible resources of activities that will be conducted during the transition period and shall describe the Contractor's plan for:

- Transition of Hardware, Software, Licensing, and resources
- Knowledge and skills transfer
- The Contractor will provide detailed project documentation, in compliance with Chapter 60GG-1, F.A.C., for the end of term transition component of the contract which will include:
    - Project Charter
    - Project Deliverables
    - Project Schedule with start dates, end dates, tasks, dependencies, and critical path.
    - Work Breakdown Structures
    - Resource Plans including State resources needed for transition support
    - Risk Register and risk mitigation strategies.
    - Maintain action item logs, issue logs, and decision logs
    - Budget
    - Communication Plan
    - Stakeholder List
    - Weekly Status Reports to include project status, variance, risks and issues, changes, milestones, deliverables, and major tasks.
    - Requirements traceability matrix
    - Project Management Plan to include:
        - Resource management plan
        - Schedule management plan
        - Communication management plan
        - Change management plan
        - Quality management plan
        - Risk and issue management plans
        - Deliverable acceptance plan
        - Cost management plan
- The Contractor will provide a detailed Resource transition plan

THIS SPACE IS INTENTIONALLY LEFT BLANK.