ATTACHMENT A – DIR SHARED TECHNOLOGY SERVICES POLICY DOCUMENT

SOW No. 781-3-29358

Data Center Services

SOW Language for DCS Customers Seeking IT Solutions

March 2022

All Data Center Services (DCS) designated agencies are required to include DCS hosting requirements language below in Statement of Work (SOW) that include IT infrastructure as either a hosted solution or Software as a Service (SaaS) solution. The intent of this language is: 1) to give respondents a clear understanding of the requirement to use the State's DCS program public or private cloud, 2) how respondents should propose technical solutions hosted in DCS, and 3) to communicate how respondents are expected to integrate with the DCS program vendors and services throughout the life of their contract. The areas highlighted in yellow indicate places where the agency should customize the wording to fit their specific agency, situation, or SOW structure.

SOW Language:

Data Center Services (DCS) Infrastructure Requirements

The Texas Legislature, by action of House Bill 1516, 79th Legislature (Regular Session), established the foundation of a shared technology infrastructure and directed Department of Information Resources (DIR) to coordinate a statewide program to consolidate infrastructure services. Section 2054.391 requires State agencies included in the DCS program to use such services, unless otherwise approved by DIR through a Data Center Services Exemption. DIR currently has executed multi-vendor contracts to provide data center managed services for DIR Customers.

All hosted solutions offered in response to this SOW (including custom developed application, COTS, and Portal or Website managed content) must host the application or solution in the DCS program, using either public or private cloud compute and DCS managed services provided.

Respondents should comprehensively list their infrastructure or compute requirements, to be hosted in either a DCS public or private cloud, for financial review by the Texas Higher Education Coordinating Board (THECB). THECB will facilitate the process to request an estimate of the cost to host the solution within the DCS program.

If the Respondent intends to propose Software as a Service (SaaS), then the Respondent must demonstrate that the solution clearly meets the National Institute of Standards and Technology (NIST) standard definition of SaaS (NIST Definition of Cloud Computing Special Publication 800-145). The solution must be TX-RAMP certified (or equivalent substitution). THECB will be required to request and receive from DIR a DCS program exemption before a contract can be awarded to a Respondent if the solution is purchased outside of the DCS program.

More details about the DCS Vendor Contracts, Master Services Agreements (MSAs) and Statements of Work (SOWs) may be found on DIR's website at: www.dir.texas.gov.

Respondents should provide one technical solution: either SaaS or DCS hosted and managed. If your proposal is for a hosted solution, it will need to be hosted in the State's DCS program, which offers both public and private cloud hosting options. This program provides all server management functions including system administration, operating system management and patching, base security services, dedicated local area network connectivity, storage services, backup services and disaster recovery services. Respondents should indicate whether it is proposing fully managed, or semi managed DCS infrastructure hosting and compute solutions required.

Respondents are not required to estimate the cost to host within the DCS program; however, Respondents are required to provide complete technical specifications in order for THECB to estimate.

Collectively, the DCS contracts provide participating Customers mainframe and server operations, both public and private cloud services, disaster recovery, and bulk print and mail services.

DCS Public and Private Cloud Compute and Software Acquisition

As a participating entity in the DCS program, THECB is required to acquire all in-scope infrastructure compute, services, and software through the DCS program. Respondents must include complete compute and software infrastructure requirements in their response in order for THECB to estimate DCS costs.

The Successful Respondent is required to participate in the procurement process, including submitting the request for service into the DCS ServiceNow Tool, participating in the requirements gathering sessions, and validating the acquisition proposals received. Proper long-range planning is required in order to ensure compute is provisioned to meet project schedules.

DCS Process Management

The Successful Respondent will be required to participate in the defined DCS processes for incident management, problem management, change management, release management, configuration management, and request management. In the management plans described in this SOW Section 3.0, the Respondent must describe its interactions with the DCS program.

DCS Public Cloud

Industry leading public cloud services available from DIR Shared Technology Services are hardened public cloud virtual data center solutions with a focus on aligning the DCS Operating Model with Industry Best Practices, technical and security assurances, and onboarding of public cloud services through Amazon Web Services (AWS), Azure, and Google.

Leveraging Cloud Native tooling, the DCS Cloud Service model is poised to align to the value of Cloud Service Providers by evolving capabilities with investment in Service Evolution of the Public Cloud. Our expanded Public Cloud model delivers Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and SaaS services with products and tooling built for and within the Public Cloud to leverage the full benefits of Public Cloud services with the security assurances of DCS.

Sandbox Public Cloud Support

This operational model is intended for environments with use cases such as proof-of-concepts, sandbox, and lower lifecycle development and testing activities which can operate with network restrictions preventing communication with the STS Consolidated Data Centers and unsolicited inbound internet communication. Network connectivity to this environment is through a secure Customer Virtual Private Network (VPN) connection provisioned by the DCS managed service provider.

Native public cloud console access to Public Cloud IaaS services (with minimal restrictions) is available enabling customer flexibility operating in the Public Cloud.

Customers are fully responsible for services provisioned within the Sandbox support environments, with minimal Service Component Provider (SCP) support provided.

Semi-Managed Public Cloud Support

The Semi-Managed Cloud operational model is intended for environments where the Customer is responsible for operating system management and monitoring, application-level support and associated incident and change management. This environment requires connectivity through a DCS managed Direct Connect/Virtual Cross Connect (VXC) solution, delivering integration of private cloud resources with public cloud resources including STS assurances.

DCS solutions enabled for Customers include the following operational functions for the semi managed environments.

- Native Public Cloud console available with full read access to the cloud environment.
- Specific console roles can be discussed with Public Cloud Manager (PCM).
- SaaS based log aggregation services to capture, extract, transform and load pertinent security and event details from Public Cloud management environments.
- Advanced analytics and data correlation greatly extend the success of forensic research and investigation.
- Capture Azure events via Operations Management Suite (OMS) logs; AWS events via Cloud Trails and Cloud Watch; Google Cloud Platform (GCP) events via Cloud Operations Suite.
- Cloud Access Security Broker solution spanning AWS, Azure and GCP providing sophisticated analytics to identify violation of policy and combat cyberthreats.
- Utilizing the Security Instrumentation platform (SIP) to measure against cybersecurity Key Performance Indicator (KPI) and targets. Tests effectiveness of network, endpoint, and cloud controls.
- Advanced, customizable reporting with comprehensive Application Platform Interface (API) access and integration across multiple platforms.
- Endpoint protection online or offline with integration into tools such as Windows System Center for compliance and regulatory requirements and mandates.

The DCS SCP is responsible for:

- Provisioning and deprovisioning,
- Enabling Customer console and IaaS access,
- Acquiring, installing, and patching the operating system,
- Installing and maintaining antivirus,
- Backups and recovery,
- Performing Security Information and Event Management (SIEM) logging, critical watch reporting and security incident response, and
- Asset discovery and Configuration Management Database (CMDB) integration.

Fully Managed Public Cloud Support

The Fully managed Cloud operational model is intended for environments where the DCS Service Component Provider (SCP) is responsible for all aspects of the service lifecycle including provisioning, deprovisioning, ongoing operating system (OS) support, monitoring, environment maintenance, Customer incident request, change requests, and service requests. Connectivity over a new or previously existing Virtual Cross Connect (VXC) between on-premises CDC resources and cloud resources enables the extension of STS assurances to the hybrid environment.

DCS solutions enabled for Customers include the following operational functions for the fully managed environments.

- Native Public Cloud console available with full read access to the cloud environment.
- Read access to view inventory and state information of cloud resources.
- Usage and cost reporting and budget management.
- Log aggregation services to capture, extract, transform and load pertinent security and event details from Public Cloud management environments.
- Advanced analytics and data correlation greatly extend the success of forensic research and investigation.
- Capture Azure events via OMS logs; AWS events via Cloud Trails and Cloud Watch; GCP events via Cloud Operations Suite.
- Cloud Access Security Broker solution spanning AWS, Azure and GCP providing sophisticated analytics to identify violation of policy and combat cyberthreats.
- Utilizing the Security Instrumentation Platform (SIP) to measure against cybersecurity KPI and targets. Tests effectiveness of network, endpoint, and cloud controls.
- Advanced, customizable reporting with comprehensive API access and integration across multiple platforms.
- Endpoint protection online or offline with integration into tools such as Windows System Center for compliance and regulatory requirements and mandates.
- Real-time intervention, blocking, and prevention for any in-process runtime attacks, includes,

- Integration with third-party tools across the entire cloud native lifecycle.
- Web Application Firewall protecting applications in the cloud with consistent policies and management capabilities as on-premise solutions (optional).

The DCS SCP is responsible for:

- Provisioning and deprovisioning,
- Enabling Customer console and IaaS access,
- Acquiring, installing, and patching the operating system,
- Ongoing operating system (OS) support,
- Installing and maintaining antivirus,
- Monitoring and environment maintenance,
- Performing SIEM logging, critical watch reporting and security incident response,
- Backups and recovery,
- Customer incident request, change requests, and service requests, and
- Asset discovery and CMDB integration.

Platform as a Service (PaaS)

DCS managed Direct Connect/Virtual Cross Connect (VXC) will be required for integration between the CDC and the Cloud Service Provider PaaS environments.

DCS solutions enabled for Customers include the following operational functions for PaaS environments.

- Native Public Cloud console available with full read access to the cloud environment.
- PaaS access management provisioned in alignment with DCS program service responsibility matrix distinguishing Customer and service provider responsibilities.
- Read access to view inventory and state information of cloud resources.
- Usage and cost reporting and budget management.
- SaaS based log aggregation services to capture, extract, transform and load pertinent security and event details from Public Cloud management environments.
- Advanced analytics and data correlation greatly extend the success of forensic research and investigation.
- Capture Azure events via OMS logs; AWS events via Cloud Trails and Cloud Watch; GCP events via Cloud Operations Suite.
- Cloud Access Security Broker solution spanning AWS, Azure and GCP providing sophisticated analytics to identify violation of policy and combat cyberthreats.
- Utilizing the Security Instrumentation Platform (SIP) to measure against cybersecurity KPI and targets. Tests effectiveness of network, endpoint, and cloud controls.
- Advanced, customizable reporting with comprehensive API access and integration across multiple platforms.

- Endpoint protection online or offline with integration into tools such as Windows System Center for compliance and regulatory requirements and mandates.
- Real-time intervention, blocking, and prevention for any in-process runtime attacks, includes.
- Integration with third-party tools across the entire cloud native lifecycle.
- Web Application Firewall protecting applications in the cloud with consistent policies and management capabilities as on-premise solutions (optional).

The DCS SCP is responsible for:

- Maintenance and enablement of VXC and Virtual Private Cloud (VPC)/Virtual Network (VNET),
- Integration between public cloud IaaS services and PaaS service as needed,
- All cloud deployments,
- Enabling Customer console and PaaS access, and
- Asset/Service discovery and CMDB integration.

Virtual Cross Connect (VXC)

The DCS Service Component Provider (SCP) uses Megaport to provide a virtual networking solution that allows Customers to securely connect to multiple Cloud Providers without having to establish direct connections between the individual customer and Cloud Provider.

VXCs provide dedicated bandwidth for the Customer to a Cloud Provider location, including traffic segmentation. AWS and Google require one VXC per DIR Customer, whereas Azure requires two. Two VXCs are recommended for improved network resiliency.

The DCS Service Component Provider (SCP) is responsible for provisioning and management of VXCs.

Virtual Private Cloud (VPC)

A VPC is a public cloud networking construct roughly analogous to a Virtual Local Area Network (VLAN) in current Consolidated Data Centers (CDCs). It is designed to enable network and security services to the workloads that run inside the public cloud.

VPCs go by different names based on the Public Cloud provider: Google and AWS calls them VPCs, while Azure calls them VNETs. DCS prefers to use VPCs to mean the network construct used by the Public Cloud Provider.

The DCS Service Component Provider (SCP) is responsible for provisioning and management of VPCs.

DCS Private Cloud

The Data Center Services program maintains two consolidated data centers geographically separated in order to provide disaster recovery. The Texas Private Cloud (TPC) provides technology infrastructure compute and storage based on standard reference models and managed services options.

Fully-managed or Semi-managed support services are available for all compute platforms with multiple service levels.

- Consolidated Fully Managed - Premier Plus
- Consolidated Fully Managed - Premier Plus (UNIX)
- Consolidated Fully Managed - Premier
- Consolidated Fully Managed - Premier (UNIX)
- Consolidated Semi Managed - Standard
- Consolidated Limited Managed – Sandbox

The DCS program supports operating system standards that include:

- Microsoft Windows,
- Red Hat Linux,
- SUSE Linux,
- OES Linux,
- AIX (non-standard - by advanced exception approval only), and
- Oracle Linux (Enterprise Exadata and Fractional Oracle only).

Data is protected by the Dell EMC Data Protection Suite, which writes to replicated tapeless systems in the alternate data center for Disaster Recovery purposes.

All DCS compute platforms use DCS enterprise SAN storage except for the Fractional Intel VxRail hyper-converged infrastructure (HCI) that uses an internal VSAN technology.

The DCS program offers CDC virtual compute solutions for Intel (Windows / Linux), and IBM Power System Platforms (by exception approval only) based on customer business needs. See below for more information.

Fractional Intel Virtualization (Consolidated Data Center)

The Fractional Intel Virtualization solution is an Infrastructure as a Service (IaaS) providing an Intel virtualized environment based on VCE/VBlock converged infrastructure, Dell EMC VxRail hyperconverged infrastructure (HCI) or the Cisco UCS compute systems supporting Windows and Linux operating systems.

Reliability is supported with the use of VMware virtualization and high availability clustering.

Flexible configurations are available in 1vCPU and/or 2GB memory increments. Maximum limits are 500GB memory and 72vCPU for HCI or 64vCPU for VBlock.

Optionally, Customer-dedicated Cisco Intel UCS blades are supported with Customer-specified compute, memory, and hypervisor or bare metal configurations that leverage the shared VBlock or UCS infrastructure.

Enterprise SAN Storage

The DCS program provides enterprise SAN storage services using a four-tiered approach. The tiered storage methodology supports the use of various types of data storage architecture, pricing, and recovery. The solution is based on DellEMC Vmax Enterprise Storage, is protected by redundant architecture, and can be replicated to an alternate Consolidated Data Center (CDC).

Non-HCI Server SAN Storage Tiers

- Tier 0 - All SSD storage: Highest IOPS and fastest response times
- Tier 1 – Ultra high-performance storage: Generally, for very high database transactions
- Tier 2 – High performance storage: OS and production databases requiring high performance
- Tier 3 – Medium performance storage: Standard storage requirements

HCI VMware vSAN Storage Tiers

The VxRail HCI uses VMware vSAN which provides all flash storage to the hyper-converged environment. VMware vSAN is a hyper-converged, software-defined storage (SDS) product developed by VMware that pools together direct-attached storage devices across a VMware vSphere cluster to create a distributed, shared data store.

HCI Server vSAN Storage Tiers

- Tier 1 – Ultra high-performance storage: Generally, for very high database transactions
- Tier 2 – High performance storage: OS and production databases requiring high performance
- Tier 3 – Medium performance storage: Standard storage requirements

Private Cloud Managed Support Services (available for all compute platforms)

Fully Managed Private Cloud

The Service Component Provider (SCP) is responsible for all aspects of the IaaS lifecycle, including provisioning the:

- Ongoing operating system (OS) support,
- Ongoing database and middleware support (where optional services are selected),
- Hardware maintenance,
- Incident, change and Customer service requests,
- Service Catalog Requests,
- Asset discovery and CMDB integration,
- All base security functions (e.g. antivirus, patching, SIEM), and
- Optional advanced security available.

Semi-Managed Private Cloud

The Customer is responsible for OS support and all application-level support as summarized below.

SCP Responsibilities

- Provisioning
- Acquiring, installing, and patching the OS
- Installing and maintaining antivirus protection
- Performing SIEM logging, critical watch reporting and security incident response
- Performing hardware container maintenance and reboots
- Responding to incidents and Service Catalog requests related to hardware
- Asset discovery and CMDB integration

Customer Responsibilities

- OS management
- Monitoring
- Creating and managing incidents, change requests, and Service Catalog requests

Database Standards

Database management support for multiple database platforms are classified as two groups. Each platform allows for support and management of a database environment with Customer privileged access and with varied availability requirements for each unique Customer.

Standard Databases

- Oracle
- MS SQL
- MySQL
- DB2

Non-Standard Databases

- Sybase
- Informix
- Adabas

Oracle Database Offerings

Enterprise Exadata

Enterprise Exadata is an option for Oracle Real Application Cluster (RAC) databases requiring high performance and high availability. Enterprise Exadata is a shared Oracle engineered system that provides an isolated multi-tenant environment. Enterprise Exadata provides virtual machine clusters

consisting of two Oracle virtual machines with a minimum configuration of 4 cores and 64 GB RAM each and up to 9600 GB of storage and can be scaled up with additional cores, memory, and storage.

Exadata Configuration Options	Cores	RAM	Storage (GB)
Enterprise Exadata VM Cluster Small	4 + 4	64 + 64	9600
Enterprise Exadata VM Cluster Medium	6 + 6	96 + 96	14400
Enterprise Exadata VM Cluster Large	8 + 8	128 + 128	19200
Enterprise Exadata VM Additional cores (2+2)	2 + 2	32 + 32	4800
Enterprise Exadata VM Additional RAM (8 GB + 8GB)	-	8 + 8	-
Enterprise Exadata VM Additional ASM Storage 512 GB	-	-	512

Enterprise Exadata Minimum Oracle Database Software and Option requirements:

- Oracle Enterprise Edition
- Oracle Real Application Clusters (RAC)
- Oracle Diagnostics Pack
- Oracle Tuning Pack
- Oracle Database Vault
- Oracle Advanced Security
- Database Lifecycle Management Pack
- Oracle Cloud Management Pack
- Oracle Partitioning

Fractional Oracle

Fractional Oracle is a potential refresh target for small databases and Oracle applications. Fractional Oracle alleviates the software licensing issues with running Oracle Database software on VMware because it allows for sub-capacity licensing on Intel. It also provides better scalability and resiliency than bare metal servers. Fractional Oracle runs on the same converged infrastructure hardware (VBlock Cisco blades) as Fractional Intel and takes advantage of existing support resource units. However, Oracle Linux KVM is used as the virtualization software instead of VMware. Fractional Oracle supports Oracle Linux, RHEL, and Windows virtual machine operating systems.

Minimum Fractional Oracle vCPUs is 2 and can be scaled in increments of 2 to a maximum of 60 vCPU. Virtual memory can be allocated in 2 GB increments up 500 GB.

Minimum Oracle Database software requirements for Fractional Oracle.

Oracle Standard or Enterprise Edition version 19c.

Oracle RAC is not required in the Fractional Oracle environment, but it is an available option for databases requiring high availability.

Database Services Support Options

The DCS Database support options provide DCS Customers with greater flexibility to support application development, release initiatives, and aggressive application business availability requirements. The DCS program uses a two-level approach to support.

Fully Managed: Maintains the level of support that has historically been provided for databases.

Semi-Managed: The Customer has the majority of privileges and responsibilities but retains service provider support for availability, monitoring, maintenance, backups, patching and upgrades.

Private Cloud Hardware and Software Currency

The DCS hardware infrastructure is refreshed on a 60-month refresh cycle. Operating software, database software, and application utility tools are required to be within *n* or *n*-1 of the currently supported versions of the software manufacturer. The Respondent is required to ensure the application software developed for ApplyTexas will support the DCS standard hardware and software platforms as described in the DCS Standard Configurations.

Incident Response

Once the Successful Respondent has determined or suspects the cause of an incident is related to a DCS infrastructure component, the Successful Respondent will log into the DCS Support Center's system to report the incident in accordance with the DCS Services Management Manual.

Functions Retained by THECB – Not Provided by Data Center Services

For clarity, the following services are not provided by DCS Service Providers. In developing your response, the Respondent should clearly understand that the requestor (agency) performs these functions as needed.

- End-user computing, including desktop, mobile, and LAN-attached multi-function devices.
- Network support, including WAN/LAN support outside of the State data centers, voice/phone support.
- Help desk (Level I – all services).
- Expert troubleshooting and support for all non-DCS services.
- Technology planning, strategies, and visioning.

- Project management.
- Disaster recovery planning and testing for all retained services.
- Business continuity planning for agency processes.
- Packaged imaging systems (scanners, servers, optical disks, etc.).
- Coordination of data center print services, including coordinating form changes with business units, volume trending.
- Data security, security design and policy development, systems access requests (directory/file, ID creation and removal, determination of access rights).
- Logical database administration.
- Application development, support, maintenance, and monitoring.
- Electronic payment processing services.
- Data import and export to the environment (FTP services).
- Reporting services.

Shared Technology Services/Customer Program Responsibilities Overview

Services	STS	Customer
Systems/Environment Monitoring		
• IaaS/PaaS (Network, Compute, Service, Storage and OS, Middleware, Database)	R	
• Application		R
Security Monitoring and Management		
• IaaS/PaaS (Network, Compute, Service, Storage and OS, Middleware, Database) - Solutions, Monitoring, Management, Patching, SIEM, CSOC (ITD/ITP, Malware, DDOS, logging). STS SIEM is for STS managed environments (IaaS/PaaS) events	R	
• Application		R
Network Provisioning and support -Direct Connect and Public Cloud Virtual networking (e.g., VPC, VNET, firewalls)	R	
IaaS/PaaS Compute, Storage and Services Provisioning	R	
Support Services		
• Incident, Request, Change, Problem, Availability, Management	R	
• IaaS/PaaS (Network, Compute, Service, Storage and OS, Middleware, DB)	R	
• Application		R
• Installation and Upgrade Support (Software Services)	R	
Service Request Management (e.g. startup shutdown services for IaaS, PaaS environment support)	R	
Event Management		

Services	STS	Customer
• IaaS/PaaS (Network, Compute, Service, Storage and OS, Middleware, DB)	R	
• Application		R
Asset & Configuration Management		
• IaaS/PaaS (Network, Compute, Service, Storage and OS, Middleware, DB)	R	
• Application - Software discovered is populated in STS CMDB. Agency responsibility for Business and relationship correlation of application data in MSI provided APM (Application Portfolio Management System)		R
Backup and Recovery	R	
Disaster Recovery	R	
Production Scheduling - Application level scheduling is responsibility of customer	R	R
Availability Management (IaaS, PaaS)	R	
Identity and Access Management		
• IaaS/PaaS (Network, Compute, Service, Storage and OS, Middleware, DB) - Privileged Access Management for STS Provider managed Id's	R	
• Application - Includes DB where Customer not choosing Optional STS DB support services		R
• Account Lifecycle Management-For respective areas of support responsibility	R	R
• Active Directory - Customer Owned AD with access granted to STS as required for delivery of managed services. Customer and SCP co-exist with responsibility for respective identities.	R	R