



**Exhibit 2.3.1**  
**Solution – Server, Storage and Data Center**  
**Modification No. 15**  
VA-180815-UC

**COMMONWEALTH OF VIRGINIA**  
**VIRGINIA IT AGENCY (VITA)**  
**SUPPLIER STRATEGY AND PERFORMANCE DIVISION**

**11751 MEADOWVILLE LANE**  
**CHESTER, VIRGINIA 23836**

## Table of Contents

### Contents

1.0 Introduction.....	6
2.0 Common Services .....	7
2.1 General .....	8
2.2 Architecture and Engineering.....	8
2.3 Operations, Maintenance, and Monitoring.....	10
2.4 Patch Management .....	17
2.5 Production Control and Scheduling (Batch) .....	20
2.6 Technical Support.....	21
2.7 Capacity Management .....	21
2.8 User Support.....	23
2.9 Integration.....	23
2.10 Personnel/Clearance Management.....	24
3.0 Assume Operations and Management of Existing Services .....	25
3.1 CESC-Based Services .....	25
3.1.1 CESC Building Operations, Management, and Maintenance .....	25
3.1.2 Server and Platform Services resident at CESC .....	26
3.1.3 Storage Services resident at CESC .....	26
3.1.4 Directory Services resident at CESC.....	27
3.1.5 Network Services resident at CESC.....	27
3.2 Agency-Based Services .....	29
3.2.1 Server and Platform Services resident at Agency Sites .....	29
3.2.2 Storage Services resident at Agency Sites .....	29
3.3 Disaster Recovery Services .....	29
3.3.1 Provide replacement facility to host Secondary Data Center-based Services .....	29
3.3.2 Operate, Manage, and Maintain existing Secondary Data Center based services.....	30
4.0 Directory Services with Identity and Access Management .....	32
4.1 Directory Services.....	32
4.2 Federated Identity Management (FIM).....	33
4.3 Delegated Authority .....	35



4.4	Certificate Authority .....	35
4.5	Multi-Factor Authentication Service .....	38
4.6	Domain Name System (DNS) Services .....	38
4.7	DNS Filtering .....	38
4.8	Network Access Services .....	38
5.0	Documentation, Analysis, and Evolution.....	39
5.1	Documentation, Analysis, and Remediation .....	40
5.2	Services Evolution.....	41
6.0	Facility Management and Operations .....	51
6.1	General Services .....	51
6.2	Cabling and Wiring Services .....	53
6.3	Security Administration.....	53
6.4	Biometric Authentication .....	54
6.5	Cages and Locked Enclosures .....	54
6.6	Video/Audio Recording .....	54
6.7	Access Card Support.....	54
6.8	Facility Environmental Requirements .....	54
6.9	Personnel and Visitor Monitoring .....	56
6.10	Remote Management.....	56
7.0	Server and Platform Services.....	56
7.1	Common Platform Services .....	58
7.2	Server Services.....	59
7.2.1	General .....	59
7.2.2	x86 based commodity Servers.....	60
7.2.3	UNIX Based Servers .....	62
7.3	Database Services.....	62
7.4	Appliance Services .....	64
7.4.1	Physical Appliance Services .....	64
7.4.2	Virtual Appliance Services .....	64
7.5	Other Platform Services .....	64
7.5.1	Virtual Applications and Utility Applications.....	64
7.5.2	Middleware Services .....	65
8.0	Storage Services .....	66

8.1	Storage Management.....	66
8.1.1	External Storage Media Management .....	69
8.2	Backup and Recovery Services .....	69
8.3	Provisioning and De-Provisioning of Storage .....	70
8.4	Security and Data Management.....	71
9.0	Network Services Associated with Server/Platform/Storage Services.....	71
9.1	General Requirements .....	73
9.2	Planning and Design Services .....	73
9.3	Operations and Maintenance.....	74
9.4	Monitoring.....	74
9.5	Network-based Appliance Services .....	74
9.6	Third Party Network Services .....	75
9.7	Network Time Services .....	75
9.8	IP Address Management Services .....	75
9.9	Data Center LAN Performance Monitoring and Management Services .....	75
9.10	Remote Access Services 9.10.1General Requirements .....	75
9.10.2	Remote Access and VPN Security.....	76
9.10.3	Remote User VPN .....	76
9.10.4	Remote User VPN (clientless).....	76
9.11	Network Switching in Data Center .....	76
10.0	Disaster Recovery Services .....	76
10.1	General Services .....	77
10.2	Disaster Recovery Planning and Testing Support.....	78
11.0	Security Functions .....	79
11.1	General Integration .....	79
11.2	Endpoint Security .....	79
11.2.1	Full Disk Encryption .....	80
11.3	Data Security .....	80
11.3.1	Enhanced Database Security (EDS) Service .....	80
11.4	Application Security.....	80
12.0	Enhanced Services 80	
12.1	Cloud-Based Services.....	81
12.1.1	Public Cloud Services.....	81

Enterprise .....	81
Environment .....	82
Disaster Recovery (DR), Backup & High Availability .....	83
Agency Off boarding .....	84
12.1.2 Cloud Solution Components.....	85
12.1.3 Cloud Optimization (Optimization as a Service).....	91
12.1.4 Unisys [REDACTED] .....	94
[REDACTED] OVERVIEW .....	94
12.1.5 Web Application Firewall .....	101
12.2 Analytics Platform Service .....	106
12.3 Electronic Records Management Service .....	108
12.4 Intentionally Left Blank.....	109
12.5 Additional Database Services .....	109
12.5.1 Base Database Support .....	110
12.5.2 Extended Database Support .....	110
12.6 High Availability Services via Multi-site Solution.....	111
12.7 VITA Customer Infrastructure Supporting Specific Application SLAs .....	112
12.8 Oracle Private Cloud Services .....	112
12.9 Secure Rack Hosting Services for Agency 3 <sup>rd</sup> Party Equipment .....	116

The Functional Service Areas below reference sections of **Exhibit 2.1 (Description of Services)** and **Exhibit 2.2 (Description of Services - Cross Functional)**. The Supplier should review that section of such Exhibits before responding to each functional area. Capitalized terms in this section may refer to section headings in the Description of Services.

Supplier should provide an overall view of the solution and operational approach to meeting the overall requirements contained in the Description of Services. The Supplier need not restate the requirements from **Exhibit 2.1 (Description of Services)** rather it should articulate how its unique solution will perform the services.

The Solution Summary must contain the following components in the order specified below.

## 1.0 Introduction

Our proposed solution balances the needs of the agencies and those of the enterprise. Achieving success requires taking over the responsibility of current systems, then developing the journey that moves VITA to a shared services model that allows VITA and its customers more choices, service transparency, and service flexibility. Unisys will collaborate with the MSI BRMs to provide each VITA Customer with the ability to move to the private or public cloud that best meets each VITA customer's security and business needs.

Unisys proposes standing up a new virtual private cloud in a new data center (DC) that has direct connections to public cloud providers. This approach allows VITA to have an actual hybrid cloud underpinned by a single cloud management platform (CMP), using cloud-brokering services with private and public cloud connectivity to enable VITA to control its consumption and overall operating expense. Unisys alone is unable to control how quickly VITA and its customers move to the public cloud because it will take a collaborative effort among the MSI, VITA Information Security Officers (ISO), MSS and other participants.

Unisys understands that the MSI ITSM tool does not include the Event Management module. Unisys CMP is made up of several components; see **Figure 1.0-1**. It includes the ServiceNow IT Operations Management suite which includes Discovery, CMDB, and Event Management. Also included in CMP is Microsoft Power BI, Puppet, and the Unisys developed Enterprise Services Bus. Unisys will implement a B2B integration between our ITSM tool instance and the MSI's SMS instance; this interface will update the MSI Configuration Management Database (CMDB) daily with discovered or changed configuration items. The MSI CMDB will be used for invoicing based on catalog items ordered by VITA customers. Unisys will work with the MSI and VITA to create catalog blueprints based on CMDB classes. Composition & Management with ITSM tool, which will be used to create the MSI ITSM catalog. Once a blueprint is tested and released to the MSI portal, VITA customers will receive a service that triggers the execution of a workflow to the appropriate approver. Once this workflow is approved, it will flow to Unisys for request fulfillment. After fulfillment of the request, the change in the Configured Item (CI) attributes will be captured through Configuration Management in Unisys' ITSM tool instance through discovery. Changes in the CI will flow from our ITSM tool instance to the MSI's ITSM tool instance, thereby completing the cycle. CI attributes such as compute utilization and data usage will be discovered and managed in the Unisys CMP. Through B2B integration, this data will be replicated in the MSI ITSM tool instance and published in reports in Power BI. The reporting data will be used to validate invoices forward to Unisys before submission to VITA. Unisys will provide data integration to the MSI's dashboard and reporting systems from Unisys ITSM tool, the Operational Data Store (ODS), and/or monitoring tools to enable visibility and SMM reporting requirements.



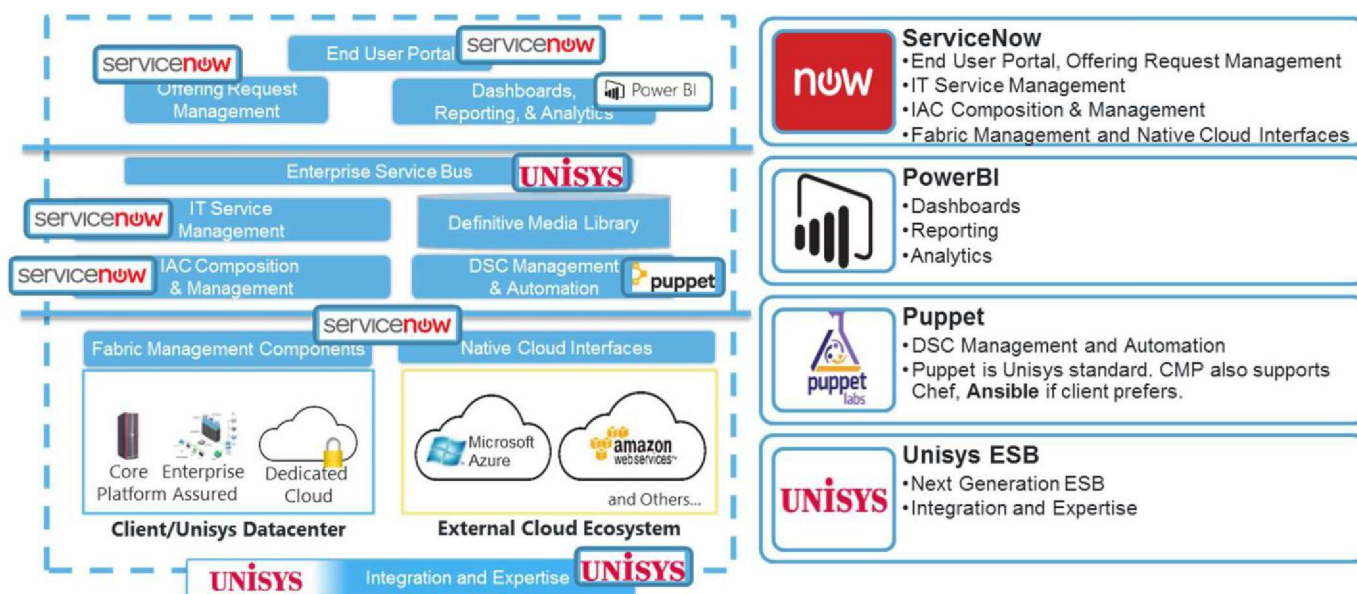


Figure 1.0-1. Unisys Cloud Management Platform.

The Unisys solution for VITA requires taking management control over the existing IT services, simplifying and standardizing the IT architecture, understanding application use, and delivering appropriate vendor-neutral new technology, underpinned by the right governance structure to help meet VITA's critical business objectives. For details, refer to *Exhibit 2.4 (Implementation Plan)*.

Working with the MSI and VITA, Unisys will produce a report that will determine the disposition of each server in VITA's environment following the guiding principles of centralization, virtualization, and innovation. The Hardware Service Charge will allow VITA to request the hardware platforms that are best suited to run its business operations now and in the future. Unisys along with our Dell partner and the involvement of VITA will propose the best hardware for each given workload. The VITA architecture board will be required to approve the infrastructure design and price.

## 2.0 Common Services

**Figure 2.0-1** is a high-level picture of VITA's Services Conceptual Architecture and the Unisys service in blue. Unisys proposed services include performing the tasks and related processes described in *Sections 1.0 through 11.4 of Exhibit 2.1 (Description of Services – Server and Storage Services; Exhibit 2.2 (Description of Services – Cross Functional)*, and *Exhibit 2.3.2 (Solution – Cross Functional)* that have associated tools and processes required for providing support and additional new services.

**Figure 2.0-2** summarizes the Services to be performed for the Server, Storage, and Data Center Systems Project.

Service Tower	Description of Services		Service Coverage
Data Center Operations and Management (DCOM)	Monitoring Automation Asset Management Capacity Management Service Management Operations CESC Critical Facilities Management Directory Services	Compute Management for Sites Storage and Backup Management for Primary, DR and Customer DC sites Database Management Support MS Windows, Linux and AIX platforms running Middleware Network Management – Router, LB, Switch, Appliance, VITA VPN, IPAM, DNS/DHCP, NTP, and replication circuit connectivity	24x7
Cross Functional Services	Service Strategy Service Design Service Transition	Service Operation Continual Service Improvement (CSI)	24x7 for Service Operations 9 hours per Business Day for the rest of the services
Program Management Office	Account Management and Governance Service Delivery Management Reporting		9 hours per Business Day

Figure 2.0-2. Services Included and Hours of Coverage.

## 2.1 General

At Commencement of Services, Unisys will assume service for console operations, monitoring, and management for data center operations, servers, storage, backup, Citrix, directory, network, and database services. Network services are for CESC and secondary data center load balancers, switches, appliances, VITA client VPN, IPAM, and NTP network infrastructure.

Unisys' Operations, Technical Support, Cross Functional, and Project Management teams will fulfill the requirements in *Exhibit 2.1 (Description of Services), Sections 1.0 through 11.4*. Our Managed Services team will perform the duties for operational and technical support related to the Servers, platforms, storage, and network. Our Security and Cross Functional teams will fulfill the requirements for data security, encryption, and compliance. Our Asset Management team will provide hardware and software life cycle-related support. Our Technical Support team will provide ongoing architecture and design support. Our Cross Functional team will also provide analytics, reports, and demand forecasts. The following sections explain how these teams will perform various services in detail.

## 2.2 Architecture and Engineering

Unisys' proposed solutions are architected and engineered to provide secure, fault-tolerant, resilient, and scalable services in the centralized DCs, VITA customer-specified facilities, and cloud services. These services are designed to support interactivity and communications regardless of activity and aligned with the security policies for VITA and its agencies.



### Architecture and Engineering in the Service Design Process

The Unisys Chief Architect and underlying architecture team will participate in MSI Chief Technology Architect-led activities to create or modify the IT Roadmap, Technical Currency and Refresh Plan, Service Design, and IT Strategy. Unisys will participate with other STSs to evaluate new technologies and service approaches so that new services are developed or changes are made to existing services. Unisys will provide knowledge and insight for our area of expertise to verify that new or changed services comply with VITA Rules including SEC501, SEC525, and IRS1075; NIST special publications; and ISO 27001. The Unisys Chief Architect will participate in MSI-led Project Portfolio Management activities as needed to understand how technology changes may affect a project schedule. Unisys use the service design process to integrate these activities into the Service Design, Service Requests, and Architecture governance standards defined in *Exhibit 2.2 (Description of Services – Cross Functional)* and *Section 2.2 of Exhibit 2.1 (Description of Services – Server and Storage Services)*. Unisys will perform the following activities to support new and updated service designs and definitions:

- Identify and assess prospective service definition opportunity
- Confirm with VITA and the MSI whether to pursue or decline the service definition activities
- Collect service requirements from requesting Customer stakeholders, or define requirements for review with VITA and the MSI
- Provide Product research and present to VITA and MSI
- Develop the service solution proposal, including evaluation of reusing existing services in the VITA Service Catalog and alternatives provided by other vendors and cloud providers
- Review the solution proposal with VITA, the MSI, and Customer stakeholders for approval
- Develop and maintain technical and functional specifications and requirements
- Submit final change requests for service catalog modifications
- Initiate a Service Transition project including documentation, service validation and testing, operational staff training, monitoring and alert configuration, configuration management, capacity management, reporting, and operational signoff before accepting customer workloads.

### Architecture and Engineering Ongoing Governance

Following the completion of service transition, Unisys architects continue to provide governance and oversight of services available to VITA and its customers. Working with our service delivery manager, our architects establish and maintain relationships with our suppliers and provide support for agencies, service tower suppliers, and other third-party vendors supporting CoV services.

### Hardware Maintenance

Unisys applies a unique approach for equipment sparing and incident resolution in the central DCs such as the CESC. Unisys will maintain an inventory of equipment for specific server configurations to provide capacity for new orders and as hardware spares in the environment. Unisys' instance of ITSM tool will discover devices attached to the network and the software running on those devices. Other unattached assets will be entered during physical inventory. The software license assets are discovered online using the Unisys ITSM tool Discovery tool, linked effectively to the assets in the MSI's ITSM tool CMDB, and tracked in the MSI's Asset Management toolset, so that the details of where the licenses are located and how they are used are known and reported. Software license reconciliation is performed with the MSI's Asset Management Tool. This means that VITA can be confident that risks related to management of software licenses are mitigated. Through integration with the MSI's SMS, asset details, including spares, will be updated in the common inventory in the MSI's ITSM tool instance. See SACM Section 5.4 in *Exhibit 2.3.2( Solution – Cross Functional)* combined with

Storage Area Network (SAN) Boot for physical servers, incidents due to hardware faults are resolved in a shorter time and allows VITA customers to maintain business operations as Unisys works with our suppliers to repair the system. Equipment is maintained and updated to current firmware and revision levels when in operation or inventory.

## 2.3 Operations, Maintenance, and Monitoring

To manage the VITA compute infrastructure for central and Customer locations, Unisys provides server monitoring and management from the CESC central operations center and Unisys Network Operation Centers in Eagan, MN, and Salt Lake City, UT, for the complete VITA server, storage, and network infrastructure in the Managed Environment. Unisys will assign a team of Unisys badged Client Engineers (CEs) to VITA.

To deliver management of the distributed infrastructure to VITA, Unisys intends to use the Unisys Data Center Operations and Management (DCOM) suite. Our DCOM suite is an integrated set of ITIL-based IT management service modules and subscription-based ITSM tool IT Operations Management technologies providing automation and remote management and support for a range of devices, including security devices, network devices, servers, storage devices, and applications built for business users. These services are managed through a single view of service performance across the IT estate. DCOM allows Unisys to deliver amalgamated remote incident management correlated across towers, providers, and geographies.

Unisys will deploy our standard monitoring tools and retain some of VITA tools as listed in *Exhibit 4.7 (Software Assets)*. Our Remote Infrastructure Management team will provide day-to-day operational support and administration of VITA DCs, Customer DCs, and the distributed server and storage infrastructure. The supported in-scope components include servers, storage, backup, databases, middleware, and network (DC LAN) and network security infrastructure. Our DCOM service enables VITA to achieve fewer responder handoffs through automated, cross-tower, cross-provider, aggregated problem management and remediation; significantly reduced time to identify, isolate, diagnose, and resolve problems, which decreases queue times; and less rework through globally leveraged expertise, facilities, and tools.

Unisys' proposal includes connectivity from the Unisys DC to secondary data center and CESC (Section 3.3.1) for our staff to take control of existing infrastructure for day-to-day operations. Connectivity includes leased lines for permanent connection and IPSec over Internet for interim connectivity. Unisys staff will have access to existing infrastructure in the secondary data center and CESC over the existing management network. During the Transition phase, Unisys will perform an assessment and make a decision on whether the existing management network has to be sized up or redesigned to provide Unisys staff access. Unisys will provide circuits between primary and secondary sites for storage and backup replication along with management. A temporary link will be implemented between the secondary data center and Unisys DR site to enable migration out of the secondary data center. Unisys has used 120 days lead time to implement new circuits. Site2Site VPN will be used for short term access until dedicated circuits are implemented.

The current [REDACTED] IP address management tool will have the assigned and available private IP addresses and ranges for the devices in the VITA enterprise. These will continue to be maintained by using the [REDACTED] toolset; Unisys will retain the same IP range wherever possible by using address translation and other OEM technologies. If retention of an IP range subnet is impossible, the related devices will be assigned new ranges that will be reflected in the IP address management systems.

The tools used for Systems Management are listed in **Figure 2.3-1**. This includes the tool name, its capabilities and functions, and key integration points. The integration points are color coded with Grey, which identifies the actual tool; Yellow, where the tool has limited integrations or will use another tool (e.g., Enterprise Service Bus or Operational Data Store) as the integration point; and Green, tools with direct integration.

Unisys support staff will have full access to the DCOM suite to have an up-to-date status of devices. VITA and Customer Architects will have access to Power BI, which allows them to create custom views of data in the ODS.

Tools	Function/Capability	MSS SIEM	Unisys Enterprise Service Bus	Unisys Operational Data Store (ODS)	MSI Service Management	MSI Configuration Management Database (CMDB)	MSI Service Catalog
	Asset and Configuration Discovery CMDB synchronization with the MSI CMDB						
	Job Scheduling						
	IP Address Management						
	Backup and Archive (Data Protection)						
	Device Hardware Monitoring & Management						
	Database Snapshot Data Masking						
	Orchestration						
	Device Hardware Monitoring						
	Device Hardware Monitoring						
	Remote Access (Console, HTTP/HTTPS, Remote Desktop, Secure Shell (SSH))						
	Software Distribution (Patch Management)						
	License Tracking Service Asset Configuration Management						
	Software Distribution (Application Packaging, Patch Management)						

Tools	Function/Capability	MSS SIEM	Unisys Enterprise Service Bus	Unisys Operational Data Store (ODS)	MSI Service Management	MSI Configuration Management Database (CMDB)	MSI Service Catalog
	Provisioning						
	Job Scheduling						
	Configuration Compliance						
	Data Center Infrastructure Management (DCIM)						
	Software Distribution (Application Packaging, Patch Management)						
	Automation and Orchestration						
	Application Performance Monitoring						
	Event & Threshold Monitoring						
	Network Performance Monitoring						



**Figure 2.3-1. System Management Tools.**

Our DCOM suite consists of three capabilities (Monitoring and Analytics, Infrastructure Availability Service, and Infrastructure Management) for the CoV:

**Monitoring and Analytics** – The monitoring service consists mainly of fault and performance management with web-based reporting. Unisys provides an automated event monitoring system using [REDACTED] and vendor-specific monitoring tools that proactively and reactively identify failures, performance issues, traffic issues, and other transient events used for the collection of detailed information required for Service Level Agreements (SLAs), reports, and invoicing. Event monitoring functions and incident control are the crucial activities in the service.

Our solution consists of both agent and agentless tools and proactively monitors the following:

- Data Center LAN performance (Latency, critical path visualization, and Performance analysis) and troubleshooting
- Network traffic and bandwidth analysis
- Switch port monitoring and device tracking
- Application/web server monitoring (health, availability, and uptime)
- Multivendor storage monitoring (performance and capacity) Application monitoring, URL monitoring, and database Monitoring and Optimization). Application Monitoring will cover the standard application services running under operating system and URL monitoring.

- Virtualization (across cloud infrastructures), and server performance (inclusive of Linux, Windows, Solaris/SunOS, AIX) - [REDACTED] can monitor all VITA platforms
- Patch Management

Unisys has provided default server monitoring service levels in *Exhibit 3.1 (Service Level Matrix)* deployed as part of the standard for initial deployment. These values may be modified after deployment as part of ongoing tuning to confirm accurate identification of threshold conditions. Our [REDACTED] solution provides comprehensive monitoring using Simple Network Management Protocol [REDACTED] polls devices using SNMP to obtain real-time performance and state information. [REDACTED] is configured to alert when a threshold or state change occurs for metrics that are also included in *Exhibit 3.1 (Service Level Matrix)*.

[REDACTED] Server & Application Monitor will be configured to monitor server and application performance and also provides real-time and historical trends in intuitive and meaningful dashboards. This data will be further fed to [REDACTED] for reporting and analytics. [REDACTED] Real Time Process Explorer monitors processes running on servers, web servers, and application servers for memory, virtual memory, CPU, disk I/O, and other definable parameters in accordance with VITA's requirements. With Real Time Process Explorer, remote management is facilitated, which means that VITA system administrators will not have to log on to a particular machine physically or remotely to run Task Manager to retrieve that machine's vital statistics. Server & Application Monitor's web console displays data for monitored and unmonitored processes, allowing VITA system administrators to diagnose server performance issues. Unisys will configure [REDACTED] database performance analyzer to provide comprehensive database performance monitoring for MS SQL and Oracle database platforms. This monitoring includes database and SQL query fine-tuning advice, identifying database problems in real time, and root cause analysis of databases. [REDACTED] Network Performance Monitor will be configured to provide monitoring of multivendor network devices in VITA's estate. The performance data captured for various parameters will be logged in Unisys' back end ODS system for further capacity and performance reporting and trend analysis.

Events identified by monitoring are configured with a severity that is based on the definitions in the MSI's Service Management Manual (SMM). Once these events are correlated, de-duplicated, and mapped to the appropriate impact and urgency definitions, Network Performance Monitor will generate incidents that are forwarded to the MSI's Service Management System so that Unisys and the MSI meet SLA requirements. Unisys will provide the MSI with input on the Event and Incident Management procedures in *Section 4.1.5, Service Operations of the SMM*.

Unisys CEs will filter and respond to events based on those definitions. As part of the Incident Management process, incidents generated from automation will be assigned to the appropriate support team. The Unisys Command Center is the main first assignment where Tier 2 remediation is performed. If Tier 2 resources cannot correct the issue, Tier 3 resources are engaged as defined in the escalation procedures outlined during transition and documented in the MSI's SMM.

During the Transition phase, Unisys will identify and establish the Event Monitoring and Severity classifications in the definitions. Unisys will maintain relevant documentation, including tower-specific documents and Incident Management that is within Unisys' scope of service, in accordance with the SMM. In the Unisys ITOM solution, incidents generated from events will be directly logged at the B2B interface and be maintained by Unisys in the MSI's ITSM tool instance. Unisys assumes that the MSI will enable and configure the established classification of events with their severities during the Transition phase.



**Infrastructure Availability Service** – Unisys uses our event management console to understand the pattern of events generated from the monitoring tools and to cross-check incidents in ITSM tool for critical events. The principal activities in the service are remote service restoration, incident management, and SLA reporting.

**Infrastructure Management** – In this service, Unisys manages DCOM input to the cross-tower problem management, configuration, and release management functionalities. The principal activities in the service include change coordination and the DCOM server operations interface with the MSI's Service Management and SMM, including problem management, change management, configuration management, release management, capacity management, and availability management.

Unisys will leverage the Customer application or business service mapping (BSM) information in the MSI's Configuration Management Database (CMDB) to understand application affinity and impact as part of the end-to-end monitoring and autoticketing activities. Although this information is not required for focusing on individual servers, it is necessary to view an Customer's application in its entirety. The service information enables Customers to understand which applications and resources are affected during incidents and changes as well as assists in the analysis to identify where services and usage must change to support ongoing business changes.

### System Operations and Maintenance

As part of operations, Unisys implements and maintains automated run books and run books based on electronic documentation. During the Implementation phase, Unisys will meet with Customer application owners to request existing copies of "automated" or "documentation-only" run books. Work Instructions or a Runbook is required for Unisys to manage the environment effectively. If there is no runbook, Unisys will work with the application owners and other service providers to create one. Unisys will then create run books for environments in which specific events require certain actions to occur. A Runbook is a best practice for managing data center systems. The Application owners(s) may not have special requirements and that will be captured in the Runbook. Unisys will work with MSI and Application owner(s) through Change Management System (CMS) process to create or update Runbooks.

### Automated Run Books

Unisys planned Knowledge Transfer activities from the incumbent will include maintaining and updating the existing run books. As Unisys would transform the environment from the current mode of operations to the future mode of operations ("FMO"), these existing run books will be maintained for VITA or Customers and align with SMM and MSI directives. Automated run books are scripts or orchestrations that occur when a particular event is triggered. An example might be a high-disk utilization alert captured by monitoring software. An automated events might be one of the following:

- [REDACTED] monitoring identifies disk volume exceeding a predefined threshold and creates an incident in ITSM tool.
- The incident ticket triggers the Automated Run Book process, which performs the following activities:
  - Retrieves detailed disk usage information for the specific drive and records details into the incident record in the MSI's instance of ITSM tool
  - Initiates cleanup actions (e.g., cleanup of temporary directories, the recycle bin, and logs as well as removal of old antivirus definition files and Windows patch files)
  - Documents cleanup results, along with cleared space details in the incident record.

### Description of the Automated Run Book Process

Unisys will implement automated scripts in our Cloud Management Platform (CMP) tools, including Puppet and ITSM tool. Unisys will follow the following three significant steps for each event that is proceeded in the automated run book:

- Gather intelligence using Event Correlation and CMP tools
- Apply knowledge from the CMDB and relationships
- Execute defined scripts with logging to meet VITA Rules

Unisys will implemented several hundred automated run books using the experience of our global operations. These run books include scripts and detailed process flows that combine the out-of-the-box product automation with the extensive knowledge and experience of our Support teams to automate activities performed by a Level 1 or Level 2 CE.

The automated run books use standard protocols (e.g., Windows Management Instrumentation and Secure Shell) and integrate them with the MSI's ITSM tool platform. The run books use an agentless deployment requiring no installation of software on the management end points. Run book security credentials are stored in the related tool's secure, encrypted vault. Upon completion of the scripts, the run book updates the ITSM incident ticket and closes the record with "closed by automation" or reassigns the incident to the appropriate resolver group to complete the run book tasks.

The run book automation also performs external notifications (e.g., sending an email or paging or calling a person or team). The automation can be coded to wait for approval of steps (e.g., rebooting a server) and written to execute tasks such as opening Change Control before processing events.

### CMP Blueprints

As described above in Automated Run Books, Unisys uses CMP to execute the scripts. Unisys will build the scripts into a blueprint. A blueprint is a set of smaller building blocks that perform one to many actions. These building blocks referred to as resource blocks within the blueprint designer allow developers to custom build a blueprint to meet a set of application and platform requirements. This includes the ability for VITA to bring their own licenses (BYOL) like Oracle. Just like installing software on laptops, a blueprint can be designed to prompt the requestor to add the license key or it can install from a known enterprise license key. The same is true for network rules, which drive governance. Blueprints can be hard coded with network firewall rules, be read from an input file from a service request or prompt the requester for the detailed information.

Unisys, along with our partners, maintain a library of resource blocks and blueprints Unisys reuses to reduce design and development time. The major driver of time for designing and deploying a blueprint is based on the complexity of the rules. Typically, Unisys recommend designing the blueprints to have as many rules as possible for the system and network to reduce the work of the requestor but Unisys must balance that with time to value and budget. Unisys will work with MSI, VITA and application owners to understand what is the right mix of automation and requestor provided information. Unisys will leverage available resource libraries in building VITA blueprints with any uniqueness for each VITA Customer. Though a blueprint very much falls into the technical category, they play a role in maintaining strong governance.

### Documentation Only Run books or Knowledge Base Articles



Unisys will leverage knowledgebase articles as a consolidated source of information that Service Desk or other STS staff use and is maintained in ITSM tool (the MSI). Unisys will house Unisys specific articles at a centralized location or store them in the ITISP Document Data Store (DDS), which is based on SharePoint, where the broader SMM is also stored. Unisys will confirm that the documentation required to support the ITISP is recorded in a common repository, as defined in the SMM. Unisys will provide 24x7 monitoring of the VITA environment from our U.S.-based Operations Centers. Unisys will use documentation-only run books for capabilities that cannot be automated. For a system or application environment, the run book consists of the list of specific events where action is required; for each unique event, it contains documentation on steps to take when an event occurs. Actions may be to perform specific technical steps or contact particular support groups. Pertinent information on actions taken will be recorded in the MSI's Service Management System. Unisys will store run books and knowledge base articles within the MSI's document repository. The run books are set up in tiers that use a client-specific top-level directory, followed by a second-level breakdown for Windows Operations Procedures, and provide the procedures for the particular application server.

## 2.4 Patch Management

Unisys follows a systematic approach of patching environments, which will start with our Security team receiving in-cycle and out-of-cycle releases from website notifications, RSS feeds, email for Microsoft, VMware, Citrix, Red Hat Linux, other VITA-used Unix distributions (e.g., Solaris and AIX), and VITA-supported databases and middleware products, including alerts from the SANS Institute or threat intelligence/ patch notifications from the MSS, Commonwealth Security and Risk Management (CSRM), or other authoritative sources (e.g., Customer ISOs). Unisys will work with MSI and the MSS on the Security Plan, which will govern how patches will be identified, evaluated, and its deployment approach whether emergency, standard or custom situations.

Unisys understands that the MSS will be performing periodic vulnerability scans and will notify the MSI and Unisys of vulnerabilities that require remediation. Unisys will follow documented SMM procedures to resolve vulnerabilities based on agreed-to threat levels, with the MSI, to understand and rate each threat and the mitigation approach to be taken per the Security Plan.

Our Security team follows the standard patching of systems using the tools across the environment. Unisys will deploy the patch management toolset as denoted in Figure 2.4-1. Unisys will work with the MSI and VITA on the change of current tools used for the VITA environment.

Following is a list of the standard tools that are used to deploy patches in accordance with VITA Rules.

Platform	OS or Technology	Standard Tool
Server	Windows	
Server	Redhat Enterprise Linux	
Server	Centos, SUSE Enterprise Linux, Ubuntu	
Server	SunOS / Solaris	
Server	AIX	
Server	HPUX	
Dell Server hardware	BIOS, Firmware	

HP Server hardware	BIOS, Firmware	
VMware	ESX, [REDACTED]	
Active Directory	GPO	

Figure 2.4-1. Unisys Standard Tools.

Unisys will run compliance reports each month to identify missing patches. Unisys will develop plans together with the MSI and VITA customers to remediate missing patches and determine when the patches can be applied.

Unisys will develop Patch Management processes as part of the SMM that detail procedures, RACI, operations guides, work instructions, and job aids to meet the requirements of patch management. Unisys will work with the MSI to verify that the procedures are complete according to SMM standards, received stakeholder review and approval, and are used to support the environment. Unisys will maintain and update the SMM procedures as part of ongoing operations.

The document will provide:

- A description of the process
- A workflow, to two levels :
  - 1st level - the outline/overview of the process showing interaction with users/initiators, interaction with other processes, interaction with already defined technical applications and the major procedures of the process
  - 2nd level – showing major procedures, departmental responsibilities, interactions, dependencies, outputs and flow control.
- The initiators of the process (triggers)
- The key outputs of the process
- The key participants in the process
- The key technology ‘touch points’ (tools/applications)
- Closure handoff criteria

#### Analyze/Categorize

Upon the release of a patch, Unisys analyzes the information to determine whether it contains specific concerns for the environment. Unisys will evaluate the vulnerability, subsequent patch, and ratings along with specific client environmental criteria. Using VITA policies and controls in addition to operational standards, Unisys will review the vulnerabilities to decide whether to recommend patching the vulnerabilities, or defer patching until the next patch cycle. To determine applicability, Unisys also uses industry-standard sites (e.g., SANS Institute and similar vendor sites).

#### Vulnerability Rating Definitions

Rating	Definition
Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.



Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

Figure 2.4-2. Vulnerability Rating Definitions.

## Change Scheduling

Once agreement is reached in accordance with VITA policies to perform a patch, Unisys submits the appropriate Change Management request with a detailed implementation plan that documents the implementation, validation, and backout steps in the MSI's Change Management System. After approval, Unisys will test the patch in a Test/DEV environment to confirm that this change can be deployed to production without issues and the patch does not cause application issues. Unisys will ask VITA Customer application teams to verify that the patch does not interfere with the applications running on the affected servers. Adequate time for testing the application will be allowed before installation to production servers. Unisys will follow the patching schedule and standards documented in the SMM. Unisys recommends allowing 1 week for testing the patch before applying it to production.

This software patch package is independent of the actual software release executable. The deployment package is created in the deployment tool [REDACTED]. Many security patches come prepackaged and do not require customizations. In rare cases, Unisys will bundle some releases into a deployment package, and a script may have to be created to customize the installation. Unisys will create the deployment package. Following are the steps for both successful and unsuccessful patch deployments:

- If the patch is successfully tested in the Test/DEV environment without issues identified, Unisys closes the change request and makes plans to deploy the patches to production.
- If the patches caused issues, Unisys initiates the backout procedure, and perform additional analysis to determine the problem's cause. If the issue cannot be remediated in the Test/DEV environment, Unisys does not deploy the patch to production.
- Once the patch is successfully validated in the Test/DEV environment, Unisys submits a new change request with a detailed implementation plan for production that documents the implementation, validation, and backout steps.
- Unisys will schedule changes following agreed to maintenance windows and MSI Change Management requirements.

Unisys will patch the VITA enterprise hardware and software infrastructure components in line with the SMM. Unisys will continue to leverage Current Mode of Operations (CMO) tools for patching of VITA's existing infrastructure components. As part of the Implementation phase, Unisys will bring our patching tools for the FMO environment. The Windows environment will use [REDACTED], the Linux and UNIX environments will use [REDACTED], vSphere environment will use [REDACTED], and storage database and backup tools will use the Original Equipment Manufacturer (OEM) native tools.

Unisys is relying on VITA to perform the following activities to support patch management:

- Define Patch Management Policies and approve requests

- Provide appropriate maintenance windows to support upgrades, patching and remediation activities

## 2.5 Production Control and Scheduling (Batch)

The Unisys Batch Scheduling and Management Service provides management and administration of production control and other batch processes in an enterprise computing infrastructure. This service delivers a flexible and process-oriented service and the required infrastructure to meet VITA's evolving business needs. Unisys uses a centralized ITIL-based Service Management model, leveraging infrastructure, processes, and people across multiple client accounts to gain cost savings and provide process standardization.

### Batch Script Management

To manage job scripts for VITA customers, Unisys will tailor our standard processes for managing job scripts during transition and document the scripts in run books for the systems. Unisys will perform the following batch script management functions as part of this service:

- Develop, test, deploy, and monitor job scripts and schedules across the platforms enrolled in the Batch Scheduling and Management Services in VITA infrastructure
- Provide a daily abort log that is available to VITA customers at the Service Portal
- Maintain at least two previous versions of scripts under version control.

### Batch Scheduling Management

Unisys will assume responsibility for batch scheduling management functions for VITA and VITA Customers. To prepare daily schedules with VITA's input, Unisys will use repeatable or unique parameters to govern dependencies, timing, sequencing, and integrity of the processing schedule. Schedule start and end times will be identified by VITA and implemented and managed by the U.S.-based Unisys Operations team. Scheduling execution is provided 24x7, and the Scheduling Department accepts ad hoc requests directly or indirectly (e.g., via MSI) from authorized end users or end-user departments. Daily cutoff times for ad hoc requests will be defined and mutually agreed. Unisys schedulers perform scheduled event stream maintenance.

Unisys understands that script corrections and reruns are expected in a Batch Management process. Our Operations team will perform corrections and reruns according to the instructions provided by VITA. Our technical writers will document these instructions for use by our Operations team. Specific rerun functions may be performed by automation, which will be maintained by the Unisys Operations team using [REDACTED]. The [REDACTED] tool will support production job schedules on VITA's Windows and UNIX platforms.

Scripting to control promotion of preproduction modules to the production environments will be developed using standards agreed upon by Unisys and VITA. To manage these migrations and promotions, Unisys will use the predefined Change Management process. In collaboration with VITA, Unisys will also develop backout scripts that take each unique environment into consideration.

### Batch Management Operations Tasks

Unisys performs the following batch management operations tasks as part of these services. Unisys will perform these tasks daily, weekly, or monthly through standard operating procedures and VITA's work instructions. Unisys will develop Batch Management processes as part of the SMM that detail procedures, RACI, operations guides, work instructions, and job aids to meet the requirements of batch management. Unisys is relying on VITA or Customers to perform the following activities to support batch management:



- Notify Unisys of schedules for VITA applications
- Participate in troubleshooting of job failures related to VITA or Customer applications

### Batch Scheduling and Management Service Level Agreements

During service implementation, Unisys will assume management of VITA's existing Production Control scheduling tool, [REDACTED], and integrate it with our DCOM and the MSI's Service Management to support ongoing operations and enable future capabilities for service requests and increased flexibility for the Customers.

Unisys assigns a Production Control Subject Matter Expert (SME) to manage production scheduling services. Schedule changes use the Service Request and Change Management processes to maintain visibility and receive required approvals. Unisys manages VITA's IT infrastructure, including job scheduling, according to SLAs described in *Exhibit 3.1 (Service Level Matrix)*.

## 2.6 Technical Support

Unisys performs technical support for servers, storage, backup, network, database, middleware, appliances, and software for the VITA DC environments and remote sites as defined in the SMM. This support includes performing the tasks and related processes described in *Sections 1.0 through 12.7* and in the *Exhibit 2.3.2 (Solution – Cross Functional)* that outline the associated tools and processes required for providing this support:

Provide all technical Support in accordance with SMM for operations including:

- Refer to *Exhibit 2.3.2 (Solution – Cross Functional)* and *Sections 2 and 7* of this document for Monitoring, reporting, capacity planning, performance tuning, configuration management and problem resolution and Root Cause Analysis (RCA) for all VITA managed systems.
- Refer to *Sections 2 and 7* for details related to Server administration, Physical and Virtual Server Support, Software Installation, Patch Management
- Refer to *Section 8* for details related to Storage and Backup management
- Refer to *Section 9* for details related to Networking Support for Servers and Storage
- Install and maintain all System Software products in accordance with the SMM.
- Provide technical advice and Support to the MSI, VITA, VITA Customer and other Supplier Application development and maintenance staffs as required.
- Provide technical advice and Support to the Application Development & Maintenance (ADM) and Database Administration (DBA) staffs as required.

The Unisys DCOM technical team will manage Installs, Moves, Adds, and Changes (IMACs), configuration changes, task scheduling, operational maintenance, power on reset (POR), capacity management, performance tuning, and root cause analysis. Unisys will coordinate with OEMs and third parties for equipment repairs and ongoing documentation for the DC environment in scope based on standard operating procedures defined in the SMM.

## 2.7 Capacity Management

Capacity Management is the ITIL process focused on verifying that the servers' capacity and performance meet current and future business demands. Unisys will analyze performance trends so that potential performance issues can be identified and resolved before the service is disrupted. Unisys proactively monitors managed servers for performance threshold violations and collects performance trending data that can be used to make performance and capacity planning decisions.

VITA will lead the design and implementation of the Capacity Management Information System (CMIS) along with Unisys capacity plans and how utilization will be updated. Unisys will take over DC LAN network, server, and storage infrastructure as-is. Unisys will use existing tools initially and Unisys deployed tools after full service implementation to determine used and required capacity for in-scope devices to determine the capacity baseline in accordance with the applications used. VITA or Customer-authorized staff must review and approve this baseline - see below.

Unisys will request a capacity forecast from VITA and the Customers to include them in FMO planning and design along with the capacity baseline. Unisys will track and control service capacities to meet forecasted demand at an agreed-upon service level performance according to the process outlined in the SMM. Unisys will also right size the infrastructure and size the target infrastructure as part of the MSI Design process (along with Availability Management) to capture the capacity plans as designed. The MSI-led design process, along with rightsizing the infrastructure for the given requirements, makes an effort to understand the business and necessary performance thresholds for monitoring and advises VITA accordingly. FMO infrastructure design will be able to serve existing and forecasted workload as well as will be modular to accommodate for future growth to meet business requirements. FMO infrastructure will be monitored constantly for performance and capacity to foster a proactive rather than reactive engagement. Unisys confirm that the components in the IT infrastructure that have finite resources are monitored and measured, and that the collected data is recorded, analyzed, and reported. As necessary, Unisys will take action to manage the available resource to verify that the IT Services that it supports meet VITA's business requirements. Unisys will provide monthly capacity reports and closely study the growth rate of the environment, which will help in forecasting the future capacity.

From commencement until new infrastructure management tools are deployed, Unisys will use [REDACTED] [REDACTED] tools to collect utilization data to understand and review future capacity changes.

Unisys will rely on the [REDACTED] monitoring tool for studying and verifying peak and off-peak utilization. Unisys will monitor in-scope device capacity and resource use as well as optimize them and VITA's investments in hardware resources.

[REDACTED] will be integrated with Object Data Store (ODS), which in turn integrates with Microsoft Power BI, which transforms data into visualizations. Our Service Delivery Analytics team uses Power BI with various visualizations for analytics. This will provide VITA with excellent capacity management capabilities (e.g., proactive analysis, trending, and forecasting of IT systems at the component level).

As part of these services, Unisys performs the following performance and capacity management functions:

- Monitoring the performance of the managed servers
- Collecting performance trending data for production servers each month from our monitoring and reporting tools
- Analyzing performance trending data periodically in accordance with the service level
- Producing a periodic capacity report based on service level, identifying capacity concerns and utilization trends in the current environment

- Reviewing the report with VITA and working to identify and remediate capacity and performance shortfalls.

The proposed Unisys standard capacity management deliverable consists of IT infrastructure-level capacity management, which includes capacity management of physical and virtual servers and storage. Capacity reporting on applications and databases are not considered in the scope at this time. The standard capacity service provides historical trending, forecasting, and exception analysis for infrastructure components.

Unisys is relying on VITA to perform the following activities to support capacity management:

- Review and Approve capacity management procedures
- Participate in the Demand Management process as further described in *Exhibit 2.3.2 (Solution – Cross-Functional) Section 3.5*.

## 2.8 User Support

Unisys Service Delivery Management and Server or Storage Support teams will provide advice and assistance for VITA- and Customer- authorized users to enable use of services, for an optimal use of production resources in accordance with the SMM.

As defined in the SMM, Unisys also provides support for application owners to perform authorized changes in the environment to meet their business or application functionality updates. Unisys will provide support and administration for various products and Application rollouts to VITA and VITA Customers.

The Unisys Remote Infrastructure Management team will provide VITA users with day-to-day operational support, advice, and assistance to perform changes for in-scope products, platforms, and applications. The MSI Service Desk team will handle Level 1 end-user requests and incidents and engage our Level 2 or Level 3 technical support team.

Each authorized VITA or VITA customer representative will have access to the standard Service Catalogs to submit a standard service request or provision a resource on the FMO infrastructure.

In the interim, until the CMP is functional and connected to Keystone Edge SMS, a service request will be created at the Service Desk and forwarded to the specific tower fulfillment team (Server, Storage, Network, IAM, DBA, or Monitoring) for completion.

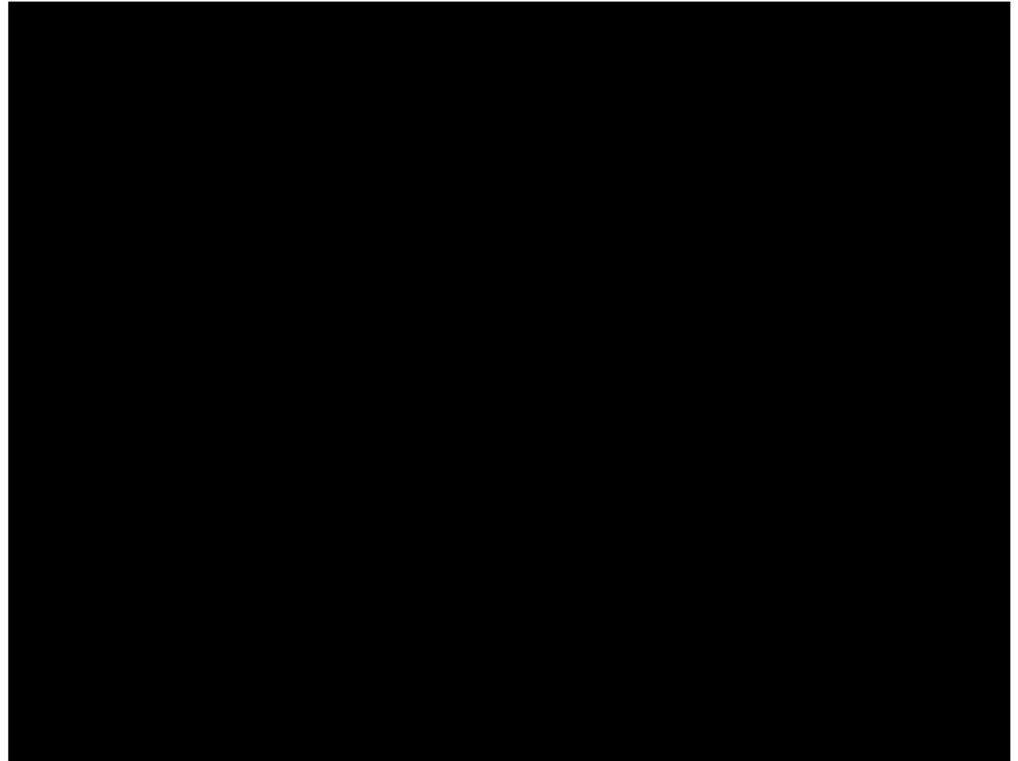
## 2.9 Integration

Monitoring and management systems are integrated in Unisys' services and the MSI's Service Management System to enable workflows and visibility to provide secure, resilient, and responsive services. Unisys also configures systems and applications to forward logs and required security alerts to the MSI and the Managed Security Services provider to support critical operations, reporting, and security alerting. **Figure 2.9-1** depicts



the tools that Unisys will deploy across VITA's environment to monitor platforms in a common way with set Event Management thresholds that will provide the MSI's Service Management System with notifications when the environment does not operate within set agreed parameters.

Working with the MSI, Unisys will enable the CMDB to receive and provide the necessary data to maintain the configuration data's currency and avoid creating islands of data in the tools environment. Unisys uses a broad set of monitoring and management tools based on the types of technologies



**Figure 2.9-1. Enterprise System Management Data Flow.** *Using the integration with the MSI ITSM, Enterprise System Management automatically creates incidents based on the events.*

required for the CoV's environment. Exhibit 4.6 (Software Assets) provides a list of the tools as well as their capabilities and upstream integration connections. To offload Unisys reporting of the integration and to report loads from the MSI Event Management System, Unisys also deploys an ODS to provide a common information repository for a single point of integration and reporting functionality.

In accordance with VITA security and operational rules, Unisys separates VITA from other clients through two methods. VITA dedicated tools deployed on-premise or in the cloud are restricted to Unisys support responsible for the VITA Program and do not contain information or connections to other clients. Management and monitoring components use role-based and data flag controls to maintain security and data separation in the tools.

During the Implementation phase, Unisys will work with the MSI to integrate the MSI System Management and Cloud Service Broker solution with our services and systems. Workflows from the MSI's System Management System and our Cloud Service Broker are used to enable automation and optimization in our CMP for interacting and providing provisioning, system administration, automation, and DevOps support to on-premise x86 servers, storage, and network in addition to cloud-based Infrastructure as a Service (IaaS) services, which includes executing DR functions. Our CMP has the ability to manage infrastructure across cloud platforms and during Implementation, Unisys will work with the MSI to determine what environments will leverage our CMP. For systems or appliances that are not integrated for automation, Unisys will work with the MSI to set up the workflows to enable the appropriate manual activities and engage where appropriate.

## 2.10 Personnel/Clearance Management

As part of VITA's onboarding activities, Unisys processes personnel providing support or having access to VITA data through a background check that meets VITA security controls, *Section 5.5* of the *MSA (Data Center – Server-Storage)* and the Standards and Guidelines detailed in the VITA Rules. The processing of personnel consists of evaluating the staffing needs, dividing those roles into job categories, which require varying levels of vetting rigor based upon access, and then vetting those resources in accordance to the standards established by both VITA Rules and Unisys' own internal requirements. All Unisys partners and subcontractors are subject to the same on-boarding process. Upon request, Unisys will provide VITA with qualifications for staff providing support services and leading the program for review. This onboarding process is aligned with the VITA security rules and the SMM to establish secure access for Unisys staff and to educate the staff on VITA business functions, operational standards, security procedures, and regulations. Unisys will apply role-based controls and separation of duties in service operation and business management to restrict use of advanced security functions and business information to authorized senior resources.

The MSI will provide Unisys with access to the Security Clearance System to record personnel results from conducted background checks through the VSP as outlined in the SMM. The MSI will provide Unisys with appropriate training in using the Security Clearance System. In addition to anything else identified in the SMM, the database will include at least the following fields: full name, company, position or title, manager name, physical location, date of clearance, additional clearances, badges issued, Customers supported, security program training, background checks, privileged access, security badge inventory, access rights, and other rights and controls to physical and logical access.

### 3.0 Assume Operations and Management of Existing Services

Unisys, with the help of a partner, will assume the operations and management of the CESC DC. Unisys has added staff to maintain operations during migration from the current incumbent. Unisys will meet with MSI and STS's collectively to determine which STS will own existing incumbent tools using *Exhibit 4.7 (Software Assets)*. Unisys has updated *Exhibit 4.7 (Software Assets)* with what tools are required to manage the current environment until they are replaced by Unisys specific toolset. There are tools [REDACTED] that Unisys will require access to during interim period.

Unisys will continue to stabilize and optimize the existing CESC and Agency DC environments through remediation and platform refresh. This will allow VITA to be well positioned to migrate to the Public Cloud or another data center by 2022.

### 3.1 CESC-Based Services

#### 3.1.1 CESC Building Operations, Management, and Maintenance

Unisys maintains SSAE 18, ISO 27001, and ISO 9000/20000 certifications on Unisys managed DCs with annual reregistrations. Unisys will incorporate the CESC into those reregistrations. Unisys follows the ANSI/TIA/EIA-942 standard for DCs and the ANSI/TIA/EIA-606 for labeling.

The CESC facility manager will confirm that the following tasks are completed (or an equivalent VITA standard). These activities will be documented in the DC procedures at the secure UnisysSharePoint and the

MSI data repository. Unisys will verify that the appropriate checks are performed according to the agreed-upon schedule:

- Monthly generator runs with load
- Quarterly:
  - Automatic Transfer Switch (ATS) checks while generators online.
  - Substation ultrasonic tests
  - Operational checks of the computer room air conditioner unit for the filter, condensing unit, compressor, and fan operating conditions; individual shutdown of equipment
  - UPS battery checks, one battery module powered off at a time
  - Coordination with the facility manager to perform above-floor cleaning.
- Semiannual Uninterruptible Power Supply (UPS) inspections
- Annual coordination with the facility manager to perform below-floor and above-floor cleaning
- UPS modules are in redundant configuration; they are never loaded to more than 45 percent
- Redundant UPS power is provided to each rack from two different Power Distribution Units (PDUs)
- Multiple generator fuel contracts
- Cooling system components are monitored by the Building Management System
- Power monitoring in place:
  - Power quality on incoming utility generators' substations
  - Power consumption meter on UPSs
- Monthly issuance of DC power and cooling statistics and report.
- Proactive reporting of resource shortages to VITA.

### 3.1.2 Server and Platform Services resident at CESC

Using the combination of the cross-functional processes detailed in the SMM, Unisys' global procedures and skilled resources, VITA, and the Customers have a strong foundation for services delivered at CESC, which will help to prevent service interruptions based on upfront planning, site preparation, and online facility data management.

The management of the DC includes receiving, installing, and decommissioning IT infrastructure, including racks, servers, storage, network hardware, and other appliances. Unisys will meet with other suppliers on a schedule to discuss and plan their upcoming activities in the DC.

The DC services focus on the full life cycle of physical infrastructure hosted in the DC. These services include activities to support the receipt, installation, break/fix, and decommissioning of equipment.

Unisys will provide day-to-day operation support, management, and maintenance of server and platform Services at CESC in accordance with the SMM procedure manuals through our Managed Compute Server Services. The compute services are designed to provide efficient managed service that addresses the challenges of a heterogeneous environment that includes x86 physical, virtual, and non-x86 (AIX, HP-UX, Sun Solaris, and Linux) platforms. Unisys will collaborate with the MSI to access current and ongoing projects initiated by Northrop Grumman for the CESC DC to provide support in accordance with the SMM and our response to Section 2.3 of Exhibit 2.2 (Cross-Functional Services).

### 3.1.3 Storage Services resident at CESC

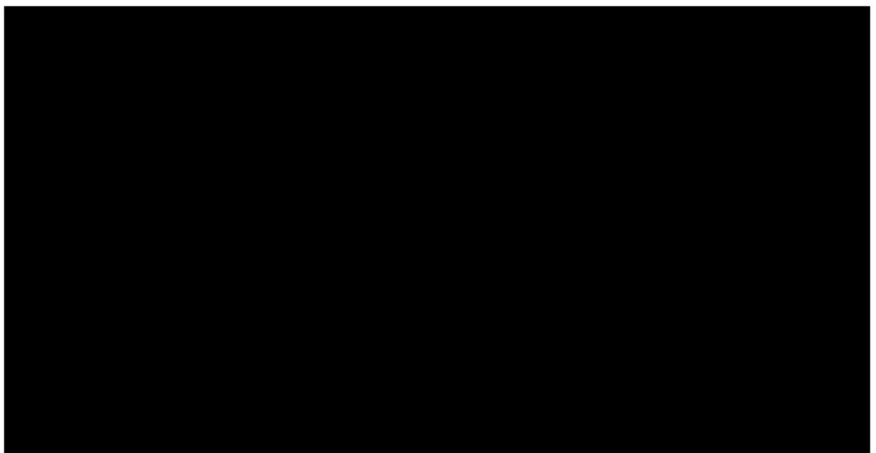


To operate manage and maintain Storage Services at CESC in accordance with the SMM, Unisys will provide remote monitoring and management of storage equipment and associated devices resident at CESC, the secondary data center, and QTS as provided in *Exhibit 4.6 (Equipment Assets)* or newly discovered storage assets from ITSM tool Discovery or physical inventory verification. The CMDB will be updated with assets that will be managed to deliver storage services to VITA and its customers to enable interdependent MSI services. Unisys will provide the MSI and VITA-approved users or VITA customers with end-to-end visibility to view real-time and historical performance statistics on infrastructure storage devices. Unisys will provide performance monitoring and tuning on infrastructure storage devices. Unisys will monitor utilization needs and efficiencies continuously and report on optimizing initiatives in accordance with the SMM. Unisys will perform maintenance according to the manufacturer's specifications and provide the MSI with documentation to verify that preventive maintenance was completed.

While the storage services reside at CESC, Unisys will operate and manage them remotely. Unisys will maintain relevant documentation that is applicable to supporting the storage in accordance with the SMM.

During transition, Unisys will create a Storage support document listing contact information (phone and email) on our SMEs as well as the Customer Storage SMEs.

The VITA application team will access the Unisys Storage Service through a Service Catalog that Unisys will build with the MSI to integrate with the underlying hardware and compute infrastructure. Our storage service staff will provide migration services for existing storage devices residing at CESC and VITA customers to bring these under the Unisys Storage Service management. As represented in **Figure 3.1.4-1**, the Unisys Storage Service will manage current and future on-premises storage landscape and public cloud storage. Refer to Section 2.4, Implementation Plan for our approach to manage the CMO and strategize the migration of workloads to FMO.



**Figure 3.1.4-1. As-Is Landscape.**

Unisys understands the requirement of completing CESC-based projects initiated by Northrop Grumman in accordance with VITA's approved project schedule and the SMM. Unisys will require understanding the requirements of these projects in the first place, and coordinated efforts and a communication plan with governance structure in place between VITA and the MSI for executing incomplete projects.

### **3.1.4 Directory Services resident at CESC**

To maintain Directory Services, Unisys follows the server and platform support functions described in Section 3.1.3. For more detail on Directory Services, refer to Section 4.0.

### **3.1.5 Network Services resident at CESC**

Unisys will operate, manage, and maintain the Network Services at CESC & DR site in accordance with the SMM. Unisys will leverage the [REDACTED] and our DCOM suite to provide remote monitoring and

management of Network Equipment at CESC & DR site in accordance with Exhibit 4.6 (Equipment Assets) as explained in Section 2.3. In CMO Unisys will utilize the [REDACTED] to monitor and manage the LAN devices in CESC & DR environments. The DCOM suite monitor and manage network devices in the new DC location to which current workload will be migrated for FMO phase. Unisys will also complete projects initiated by Northrop Grumman for the CESC DC in accordance with the customer's approved project schedule and the SMM as described in Section 2.3 of Cross Functional Services.

## **3.2 Agency-Based Services**

### **3.2.1 Server and Platform Services resident at Agency Sites**

To operate, maintain, and manage servers at Customer sites, Unisys will use remote monitoring capabilities integrated with our Event Management system along with maintenance staffing for installation, decommission, or break/fix of server assets. To manage servers and platforms, Unisys uses a consistent operating model regardless of location, as described in Section 3.1.3.

### **3.2.2 Storage Services resident at Agency Sites**

Unisys will provide remote monitoring and management of storage equipment and associated devices that reside at Customer DC and defined in Resource Unit Definition. Unisys will provide the MSI and VITA-approved users or VITA customers with end-to-end visibility to view real-time and historical performance statistics on infrastructure storage devices, as explained in Section 2.3. Unisys will continuously monitor utilization needs and efficiencies as well as report on tuning initiatives in accordance with the SMM. Unisys will perform maintenance according to the manufacturer's specifications and provide the MSI with documentation to verify that preventive maintenance was completed.

During transition, Unisys will create a storage support document listing contact information (phone and email) for our SMEs as well as the Customer Storage SMEs. The VITA application team will access the Unisys Storage Service from a Service Catalog that Unisys will build with the MSI to integrate with the underlying hardware and compute infrastructure. Unisys storage service staff will provide migration services for existing storage devices residing in CESC and VITA Customers to bring these under the Unisys Storage Service management. The Unisys Storage Service will manage current and future on-premises storage landscape and public cloud storage. Refer to Section 2.4, Implementation Plan for information on how Unisys will manage the CMO and strategize the migration of workloads to FMO.

Unisys understands the requirement of completing Customer site-based projects initiated by Northrop Grumman in accordance with VITA's approved project schedule and the SMM.

## **3.3 Disaster Recovery Services**

Unisys Disaster Recovery Services, described in Section 10.0, support VITA's needs to support business operations when a disaster is declared by the CoV CIO or agreed between Unisys, VITA, and the requesting Customer. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are defined for each Customer and application to meet the Customer's Continuity of Operations Plan (COOP) and operating model based on the MSI-managed Service Continuity Plan. VITA and Customer DR plans will be validated and updated during transition and will be maintained ongoing.

### **3.3.1 Provide replacement facility to host Secondary Data Center-based Services**

Upon a request from VITA, Unisys will work with VITA to identify an appropriate secondary data center(s) within the continental United States. Unisys will identify facilities to support VITA's requirements for hosting services, network services, disaster recovery, multi-site high-availability and other criteria.

Once an appropriate location is identified, Unisys will develop a plan with VITA and the MSI to migrate workloads, circuits and equipment to the new facility.



This will be scoped and priced as a Solution Request at the time of VITA's request.

VITA has requested solution and pricing for Secondary Data Center. The requested capabilities are documented in Exhibit 2.1: Description of Services – Server, Storage and Data Center, section 3.3.1.

Unisys will provision a new VITA secondary data center in the Ashburn Virginia, QTS Shellhorn facility.

- Unisys will build out a new data center with capabilities congruent with the new primary data center.
- Data Center Interconnects will be provided between the primary and secondary data centers.
- SAN Tier 1 Storage Replication will be enabled in both directions so DR workloads in either data center are protected at the other data center.
- NAS TIER2 filesystem replication will be enabled in both directions so NAS Tier 2 data in either data center is protected in the other data center. NAS Tier2 subscribed to DR will be configured for alternate data center network connectivity for DR testing or actual DR event.
- The design will be optimized to provide a compact infrastructure. While mirroring the primary data center capabilities, the secondary data center will have smaller floor space and rack capacity.
- A new VMware private cloud will be built in the secondary data center but with smaller total capacity.
- The new VMware private cloud platform will be configured to support multi-site and hybrid cloud scenarios.
- The existing Oracle Private Cloud at the DR center will be relocated to the secondary data center. After migration to the new secondary data center the Oracle Private Cloud infrastructure will be able to support high availability for Oracle databases, not just DR.
- Existing services at the DR center that are required in the secondary data center will either be relocated or recreated in the secondary data center.
- Unisys will work with the MSI and other affected STSs to coordinate the integration of all solutions.
- Unisys will provide reasonable assistance to other STSs and 3<sup>rd</sup> party providers in relocating or recreating their services at the secondary datacenter as may be required.
- Unisys will assist VITA in moving the VITA AIX environment from the existing DR site to the secondary data center.
- Unisys will assist Extranet Customers with moving or re-provisioning their network connections to the new data center.
- New cross connects will be established to support VITA infrastructure or movement of existing Extranet connections or new extranet connections under the "Cross Connects – All Data Centers" resource units.

### 3.3.2 Operate, Manage, and Maintain existing Secondary Data Center based services

For the existing DR services, Unisys proposes a solution to take over responsibility for the current systems and lay out a journey that moves VITA's DR infrastructure to a shared services model that supports VITA's future business needs. Unisys will collaborate with the MSI and VITA to facilitate a smooth transition of Services from the incumbent and take over support of the secondary data center infrastructure and platforms.

The new DC and secondary data center will be connected to each other with redundant 10G fibers for DR replication and backup. The secondary data center will have a 1G Internet connection; the new DC will have two of these connections. More details in table below:

Point A	Point B	Link Type	Link Specs	Bandwidth	Qty	Projected Duration

Figure 3.2.2-1 depicts the links between the DC and the secondary data center. Unisys will also evaluate Public GovCloud for compliant x86 platforms and move workloads after standardization, rightsizing, and consolidation. Unisys will provision new server and platform assets and Services in coordination with the MSI as requested by VITA and its customers.

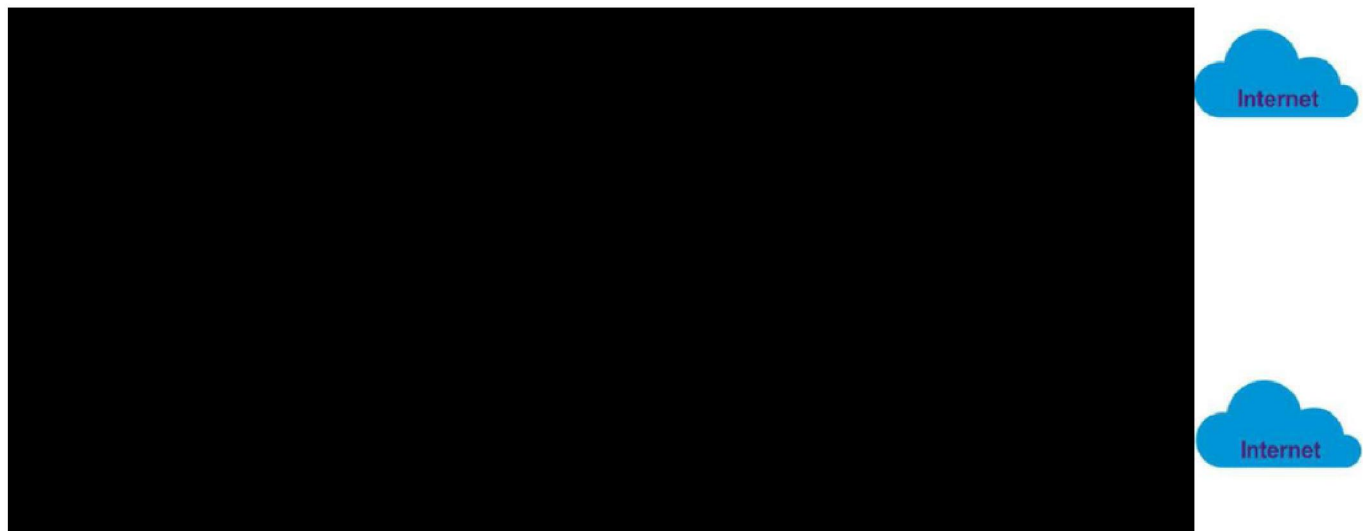


Figure 3.3.2-1. Facilities and Connectivity.

## 4.0 Directory Services with Identity and Access Management

In compliance with VITA Rules, Unisys will continue to support and optimize Directory Services, Identity Federation and Identity and Access Management (IAM) for VITA that provides services to other Customers and CoV customers in concert with MSI providing Identity Access Management governance.

### 4.1 Directory Services

Unisys understands that Directory Services are mission critical to VITA for on-premise and cloud-based applications. Unisys will adhere to the rules and policies set forth by VITA and other responsibilities listed in *Exhibit 2.1 (Description of Services)*. Unisys understands that VITA has an internal and external directory structure. Unisys will manage both directories.

**Figure 4.1-1** lists the services that our Active Directory team will perform for VITA and VITA Customers.

Administration & management	Maintenance
<ul style="list-style-type: none"> <li>• User Management               <ul style="list-style-type: none"> <li>◦ Creation, Modification &amp; Deletion</li> <li>◦ Grant &amp; Revoke Access</li> </ul> </li> <li>• Administering Domain and Forest Trusts               <ul style="list-style-type: none"> <li>◦ Explicit trusts, Creation &amp; Configuration</li> </ul> </li> <li>• Administering Windows Time Service               <ul style="list-style-type: none"> <li>◦ Configuring a time source for the forest</li> <li>◦ Configuring Windows-based clients to synchronize time</li> </ul> </li> <li>• Administering SYSVOL               <ul style="list-style-type: none"> <li>◦ SYSVOL replication</li> <li>◦ Reducing SYSVOL/GPO size</li> </ul> </li> <li>• Administering the Global Catalog               <ul style="list-style-type: none"> <li>◦ Planning and deploying GCs</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Administering the Active Directory Database               <ul style="list-style-type: none"> <li>◦ Relocating Active Directory Database Files</li> <li>◦ Returning Unused Disk Space from the AD Database to the File System</li> </ul> </li> <li>• Administering Domain Controllers               <ul style="list-style-type: none"> <li>◦ Perform tests to confirm DC health</li> <li>◦ Monitoring AD health</li> <li>◦ Hardening DCs</li> </ul> </li> <li>• Administering Group Policies               <ul style="list-style-type: none"> <li>◦ Design and Deploying Group Policy Objects</li> <li>◦ Testing Group policy settings</li> <li>◦ Isolating Group Policy issues</li> <li>◦ Backup and Restore of GPOs</li> </ul> </li> </ul>

**Figure 4.1-1. Active Directory Service to be Performed by Unisys.**

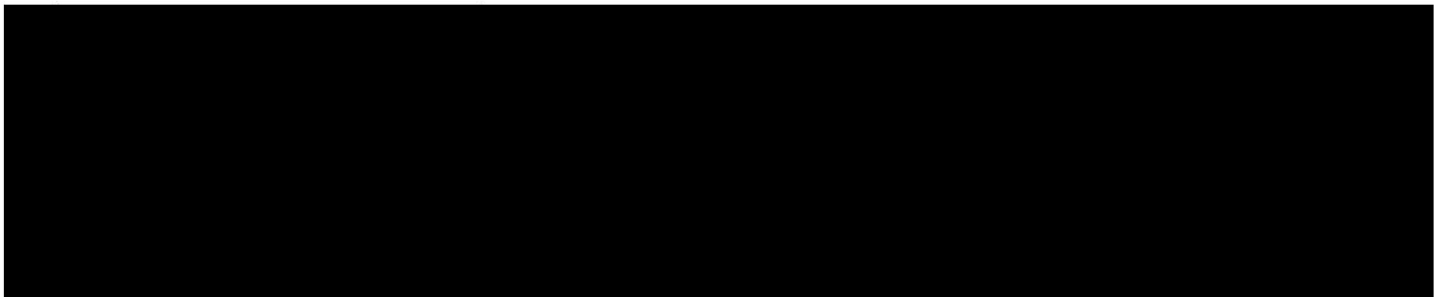
Unisys is relying on VITA, end users, or MSI Service Desk to perform the following activities to support directory services:

- Utilize self-service for password resets
- Utilize self-service to unlock user accounts
- Provide weekly maintenance windows appropriate to support upgrades, patching and remediation activities

### Optimization and Steady State Operation



Following service commencement, Unisys will work with VITA and the MSI to optimize and integrate the directory services to meet VITA's currency needs following the methodology shown in **Figure 4.1-3**.



**Figure 4.1-3. Directory Services Optimization Methodology.**

Unisys understands that the current Directory Services architecture supports trust relationships with Customer Domain Controllers. The optimization of Directory Services will continue to support trust relationships for Windows 2000 and newer.

#### **Directory Services Monitoring**

Unisys will use the [REDACTED] Server & Application Monitor component to provide intuitive dashboards to monitor the status and performance of VITA's AD and LDAP servers. Active Directory Monitoring helps obtain optimum availability and performance. Our toolset monitors key metrics including:

- Directory Services: provides that addresses, email, and phone contacts are always in sync.
- Service Outages: Alerts on each domain controller are monitored to avoid any type of service outage.
- Critical Processes: Critical processes monitored to provide availability for processing all requests.
- Domain Controller Utilization: Monitor resource utilization (CPU, Memory, Disk).
- Replication: Monitor for failures and/or slow network sync.

While Unisys plans to eliminate various [REDACTED] toolsets currently used to monitor AD and LDAP logs, Unisys understands the need to maintain existing tools during the transition.

#### **Directory Services Operations**

Unisys will leverage VITA's current investment in IAM toolsets including Okta from the Messaging Supplier. With the Okta platform, VITA can connect to many federated identity providers, rapidly onboard Customers and customers to customers' applications with minimal effort, and secure its connections with standards-based federation. Leveraging the existing investment eliminates the need to purchase additional tools and licenses.

Unisys will take over responsibility of all Admin rights for Okta VITA instance and will provide Messaging Supplier with necessary Admin control to manage its scope of services for Google and other messaging services. Unisys will coordinate Okta license subscriptions with the MSI and the Messaging Supplier and use the Okta Universal Directory product as the main identity store for the approximately 59,000 users [REDACTED]. Over time, Unisys will extend the use of Okta [REDACTED] to streamline the provisioning and management of external users while simultaneously reducing the cost of overhead.

## 4.2 Federated Identity Management (FIM)

Unisys understands that VITA desires to increase CoV-wide security by providing seamless access to government systems. The result will enhance citizen services by delivering federated access to VITA systems by internal and external entities. It will be crucial during Implementation for Unisys and the MSI to clearly delineate roles and responsibilities for these services. Unisys will maintain the production system, architect and design (with VITA review and approval), and implement a new CoV-wide federated identity management solution leveraging VITA's existing FIM platform. VITA will receive rapid benefit realization due to Unisys proven processes and technologies paired with existing VITA vendor relationships.

Unisys understands that business drives technology while technology enables VITA to meet its goals and objectives. The key to delivering secure federated identity management solutions requires understanding the requirements of internal and external users and the mandatory security regulations for driving a sound governance framework. the MSI manages the governance process for VITA, and Unisys will collaboratively work to confirm that governance workflows are seamless and secure, thereby removing potential impact on users due to outages.

VITA will benefit from the proven relationship that Unisys has with Okta, Okta's relationship with [REDACTED]. VITA currently owns [REDACTED] and Okta (from Message Service Contract). Unisys will provide Okta directly and coordinate take over based upon annual license expiration in order to provide SSO for all VITA applications.

Okta Components used in VITA	Services used by Unisys
Universal Directory (UD)	<p>Unisys will use Okta's UD to transition [REDACTED] and [REDACTED] as the single authoritative directory.</p> <p>UD will also be used to consolidate any other VITA external and/or legacy domains into the existing [REDACTED] and [REDACTED]</p>
Single Sign-On	<p>Unisys will leverage SSO to provide VITA users with access to secure resources in Google Suite, Office 365 and current on-premises applications, VITA applications on the public cloud or existing agency-managed public cloud applications, and approved third-party public cloud-hosted applications.</p>
Okta Adaptive Multifactor Authentication	<p>Unisys delivers Adaptive Multifactor Authentication (MFA) as part of the Okta platform and will deliver it to VITA as part of our core identity service.</p>

Unisys's vision is to collaboratively work with the MSI and providing Okta directly to integrate these toolsets to provide a solution to VITA for governance workflow and ability to operate and administer FIM enterprise wide. The Unisys solution leverages VITA's current investment Okta (SSO) to replace [REDACTED]



██████████ without the need for dedicated servers or firewall changes, which can minimize VITA’s on-premises footprint.

To verify that identity and access requirements are managed on Day 1, Unisys will use the following three-phased approach:

- **Baseline:** Maintain the current federated services which are ██████████ and Okta.
- **Optimize:** Work with the MSI to identify opportunities to improve compliance requirements, user experience, operational effectiveness. Improve integration with external environments and business applications.
  - **Transition/Enhanced Services:** Transition VITA to a new federated identity architecture that pairs ██████████ with Okta. ██████████ will enable the MSI to manage identity governance while having visibility to identify risks and compliance by using advanced analytics. Okta will bring Single Sign-On (SSO) to VITA.

On the path to a future state of identity, VITA users can expect to enjoy a new set of outcomes. Fulfilling these requirements and enjoying this new future state require a new approach to identity that provides speed of access and agility, faster time to value, and lower operational cost. When looking at CoV’s internal access for employees and contractors and external access use case scenarios, Unisys finds that some common architecture and operational flows can potentially gain benefit from consolidated operations. Consolidating the architecture and operational flows provide several important outcomes such as the following:

- **Speed of access and organizational agility** – This provides faster access to applications for CoV and external users as well as giving VITA the agility to shift application focus as required
- **Time to value and application delivery** – A shorter time to value enables VITA to lower costs for a project and manage a wider portfolio of applications with the same operational structure and cost
- **Lower operational cost for the business and technology operations** – When executing this new identity future state, VITA experiences lower operational cost through shorter application delivery times, lower maintenance cost, and lower user operations costs (self-service password management).

When mapping these outcomes, a series of capabilities are identified, including Identity and Application Provisioning, Global User Authentication with Multi-Factor Authentication (MFA), and Attribute-Based Application Access. Okta and ██████████ specifically provide an operational nexus where these easily operate and deploy with the FMO already described, are easy to manage, and have a delightful user experience. To better describe the operational separation between Okta and ██████████ the following list outlines the expected operational execution.

██████████	Okta
<ul style="list-style-type: none"><li>• Identity Governance</li><li>• Identity Administration</li><li>• Identity and Risk Analytics</li><li>• Compliance Management</li><li>• Privilege Access Governance</li><li>• Application Access Governance</li></ul>	<ul style="list-style-type: none"><li>• SSO</li><li>• Mobility Management</li><li>• Adaptive MFA</li><li>• Universal Directory</li></ul>

The ██████████ and Okta solutions operate as two tightly coupled components for a single set of identity capabilities already described. In this technical architecture, ██████████ continues to focus on operational



workflows, and Okta focuses on the operations and administration of the attributes as well as manages requests for access to the applications using the defined Application Programming Interfaces (APIs) and plugins in Figure 4.2-1.

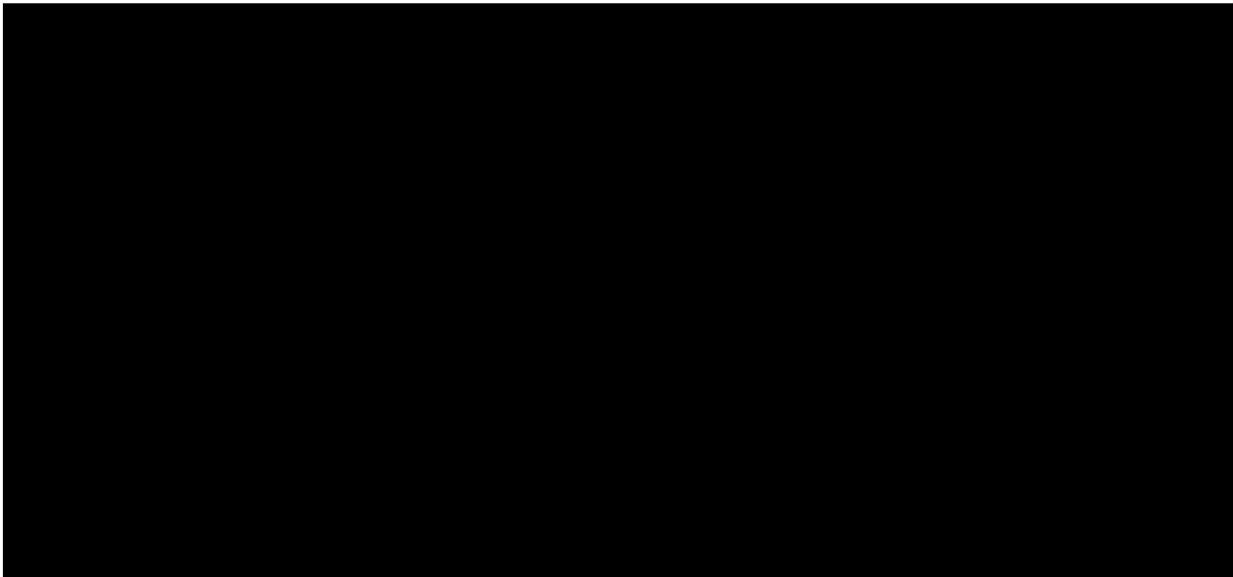


Figure 4.2-1. [Redacted] and Okta Technical Architecture. API and workflows enable provisioning and compliance management.

4.3 Delegated Authority

In compliance with VITA Rules, Unisys will provide the functionality for VITA-approved users to have delegated rights to create, change, disable, or delete accounts or customer-specific groups in their domains. Unisys will coordinate with the MSI and the Messaging Project Tower in leveraging Okta or current tool in place.

Okta provides several role-based access Administrator permissions. Depending on the role, administrators (VITA-approved users) can perform maintenance operations such as creating an account, looking up an account, unlocking an account, and resetting passwords. Activities that are performed through the Okta service are logged and available for reports and audit activities. Unisys will provide training material for VITA users with delegated authority.

4.4 Certificate Authority

The CAs are entities that issue certificates. They establish and verify the authenticity of public keys that belong to people or other certification authorities, and they verify the identity of a person or organization that asks for a certificate. Utilize MSS provided certificate management system to monitor certificate status.

CA Monitoring

- Monitor the PKI infrastructure.
- Monitor the availability of the issuing CA's.
- Monitor the Certificate Authority related services on the issuing CAs.
- Monitor the availability of the Certificates, CRL, AIA & CDP information published as captured in Figure 4.4-1.

Category	Item	Monitoring	Annotations
----------	------	------------	-------------

certificate	Root CA certificate	availability, validity	local certificate store
certificate	Issuing certificate	availability, validity	local certificate store
certificate	OCSP responder certificate	availability, validity	local certificate store
certificate	Root certificate	availability, validity	HTTP AIA
certificate	Issuing certificate	availability, validity	HTTP AIA
CRL	Root CRL	availability, validity	HTTP CDP
CRL	Issuing CRL	availability, validity	HTTP CDP

Figure 4.4-1. CA Monitoring.

Monitor the following Event IDs on the Certificate Authority servers.

#### Microsoft Windows® Security Auditing

Current Windows Event ID	Potential Criticality	Event Summary	Audit Filter Required	Description
4873	Medium	A certificate request extension changed. Request ID: %1 Name: %2 Type: %3 Flags: %4 Data: %5	Issue and manage certificate requests	If this functionality is not used by the CA, it may indicate tampering with a request
4874	Medium	One or more certificate request attributes changed. Request ID: %1 Attributes: %2	Issue and manage certificate requests	If this functionality is not used by the CA, it may indicate tampering with a request
4882	High	The security permissions for Certificate Services changed. %1	Change CA security settings	May indicate an attacker granting permissions for other accounts to enroll.
4885	High	The audit filter for Certificate Services changed. Filter: %1	Change CA security settings	May indicate an attacker disabling monitoring in an attempt to cover their tracks prior to certificate activities.
4887	Medium	Certificate Services approved a certificate request and issued a certificate. Request ID: %1 Requester: %2 Attributes: %3 Disposition: %4 SKI: %5 Subject: %6	Issue and manage certificate requests	Issuance of certificates that contain usages that allow the owner to perform privileged operations (Enrollment Agent, Code Signing etc.) or certificates issued to VIP users should be monitored.
4888	Medium	Certificate Services denied a certificate request. Request ID: %1 Requester: %2 Attributes: %3 Disposition: %4 SKI: %5 Subject: %6	Issue and manage certificate requests	

Current Windows Event ID	Potential Criticality	Event Summary	Audit Filter Required	Description
4890	High	The certificate manager settings for Certificate Services changed. Enable: %1 %2	Change CA security settings	May indicate tampering with permissions with what users are able to enroll on behalf of other users, commonly used to issue smart card certificates.
4891	Medium	A configuration entry changed in Certificate Services. Node: %1 Entry: %2 Value: %3	Change CA configuration	Can be used to monitor for changes to Policy/Exit modules on the CA or configuration of CDP/AIA extensions.
4892	Medium	A property of Certificate Services changed. Property: %1 Index: %2 Type: %3 Value: %4	Change CA configuration	Can be used to track changes to Key Recovery Agent configuration
4896	High	One or more rows have been deleted from the certificate database. Table ID: %1 Filter: %2 Rows Deleted: %3	Issue and manage certificate requests	May indicate an attacker covering their tracks after issuing certificates.
4897	Medium	Role separation enabled: %1	Change CA security settings	If role separation is used, this can be used to trigger an alert if the expected configuration changes.
4898	Medium	Certificate Services loaded a template. %1 v%2 (Schema V%3) %4 %5 Template Information: Template Content: %7 Security Descriptor: %8 Additional Information: Domain Controller: %6	Change CA security settings	Alert if templates that are not expected on a CA are loaded.
4899	Medium	A Certificate Services template was updated. %1 v%2 (Schema V%3) %4 %5 Template Change Information: Old Template Content: %8 New Template Content: %7 Additional Information: Domain Controller: %6	Change CA security settings	Alert if the certificate templates are updated/changed.
4900	Medium	Certificate Services template security was updated. %1 v%2 (Schema V%3) %4 %5 Template Change Information: Old Template Content: %9 New Template Content: %7 Old Security Descriptor: %10 New Security Descriptor: %8 Additional Information: Domain Controller: %6	Change CA security settings	Alert if the ACL's of the certificate templates are updated/changed.

Figure 4.4-2. Microsoft Windows® Security Auditing.

## Log: Microsoft-Windows-Certification Authority

Current Windows Event ID	Potential Criticality	Message
15	High	Active Directory Certificate Services did not start: Version does not match certif.dll.
55	Medium	Active Directory Certificate Services unrevoked the certificate for request %1 for %2.



60	High	Active Directory Certificate Services refused to process an extremely long request from %1. This may indicate a denial-of-service attack. If the request was rejected in error, modify the MaxIncomingMessageSize registry parameter via certutil -setreg CA\MaxIncomingMessageSize <bytes>. Unless verbose logging is enabled, this error will not be logged again for 20 minutes.
95	High	Security permissions are corrupted or missing. The Active Directory Certificate Services may need to be reinstalled.

Figure 4.4-3. Microsoft-Windows-Certification Authority.

## 4.5 Multi-Factor Authentication Service

Unisys will coordinate with the MSI to provide support of existing [REDACTED]. Unisys will coordinate with the MSI's [REDACTED] and [REDACTED] solution together with VITA's approval to migrate the entity information. Unisys will provide the tokens, the rules and processes, and actual approvals; and Unisys will manage the tokens and services in accordance to VITA requirements.

To provide a mechanism to enforce MFA (e.g., one-time password, time-synchronized token codes) for CoV vendors, contractors, and business partners, Unisys will use Okta, which provides the capability to require MFA based on access policies such as role and location. This multifactor feature includes soft tokens, hard tokens, security questions, and Short Message Service tokens. Okta provides secure, flexible MFA built in to its service and can also integrate with third-party MFA solutions. Designed to protect against phishing attacks, stolen passwords, and shared credentials, Okta's MFA solution provides the highest security and simplest administration possible. Okta's native multifactor options can be administered centrally in an integrated way, or Okta will integrate with existing third-party multifactor solutions [REDACTED].

## 4.6 Domain Name System (DNS) Services

Unisys will take over the existing [REDACTED] system at VITA that has been recently refresh to maintain the CoV Domain Name Service. At Commencement of Services, Unisys will assume service operations for the existing [REDACTED] for internal or external DNS, DNS resolution, maintenance of domain record entries, DNS/DHCP integration, and other responsibilities listed in *Exhibit 2.1 (Description of Services)*.

## 4.7 DNS Filtering

As a part of the IP Address Management (IPAM) solution managing DNS, it will accept threat feeds from multiple sources from MSS. Based on these feeds, Unisys will provide DNS filtering using the advanced security capabilities in [REDACTED] platform. Using a common platform reduces the risk from updates and improves security to servers and end users by applying filters at the source of DNS requests in addition to end-user web proxy services. Unisys security also reviews the queries, monitors them for anomalous behavior, forwards events to the MSS Supplier's Security Information and Event Management (SIEM) and processes incidents through the security incident process defined in the SMM. Unisys will work with MSS to determine what types of DNS events should be forwarded to the SIEM.

## 4.8 Network Access Services

The Directory Services team will provide remote Authorized User authentication and accounting service using the [REDACTED]. As part of [REDACTED] management and support, Unisys will use Active Directory as the backend Authorized User Directory for authentication and accounting purposes. Users and Groups will be

added and deleted as the Authorized User authentication information changes in the Active Directory. Unisys will implement [REDACTED] to integrate with Secure Sockets Layer (SSL) Virtual Private Networks (VPNs) to provide SSO [REDACTED]



[REDACTED] Figure 4.8-1 demonstrates how [REDACTED] will work:

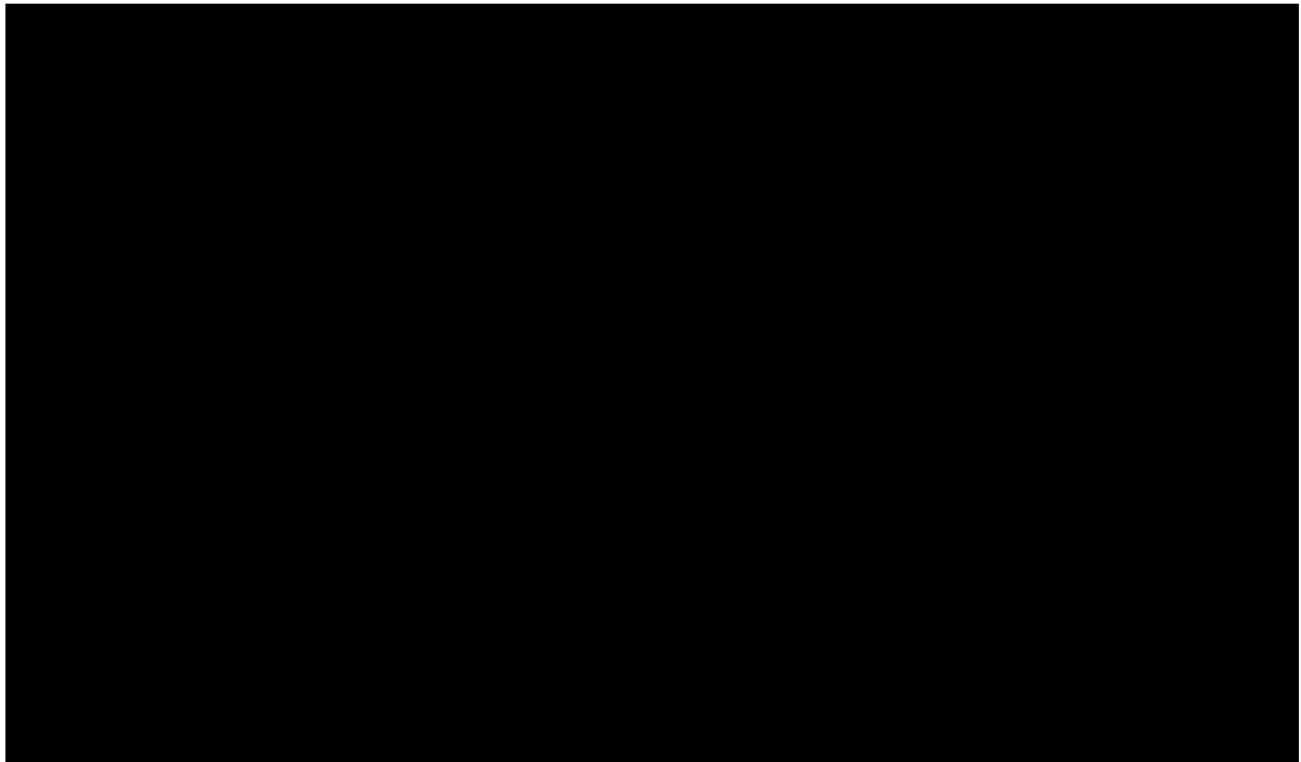


Figure 4.8-1. [REDACTED]

## 5.0 Documentation, Analysis, and Evolution

Unisys recognizes that maintaining current services and operations is important. During the Implementation Phase, Unisys will take over operations and support of the current environments as described in [\*Exhibit 2.4 \(Implementation Plan\) section 2.0.\*](#)

During the Implementation phase, Unisys will apply an integrated implementation and evolution methodology based on five phases (Discover, Analyze, Strategy, Plan, and Innovate) to identify and understand CESC's and Customers' IT environments and operations. Unisys will use these five phases to develop a roadmap and plans for successfully assuming daily operations of the current environment, updating and modernizing the IT services and hosting options, and optimizing services to align with Customers' current and future needs. Based on the requirements in [\*Exhibit 2.1 \(Description of Services\), Section 6.0.\*](#) Unisys proposes the QTS, state-of-the-art, data center in Richmond to host VITA's server, storage, and directory services. It will also provide access to AWS and Microsoft Azure services to provide increased flexibility in hosting options, modern facilities supporting industry and regulatory standards, and improved business continuity.

## 5.1 Documentation, Analysis, and Remediation

During the Implementation phase, Unisys will assess the VITA environment and DCs using several workstreams as described in *Exhibit 2.4 (Implementation Plan)*. These workstreams include the following.

- **Physical Inventory** – Perform a physical inventory of the infrastructure at Customer and Primary data center sites to document the physical environment and record the requisite data in the CMDB and other data repositories
- **Facility Assessment** – Review CESC' environment and operations to understand the current status and develop recommendations for improvements and optimization
- **Automated Discovery** – The ITSM tool automated discovery tool will discover the in-scope devices in the network and update the CMDB with the information

As part of the Physical Inventory and Facility Assessment Unisys will evaluate the current environment, operations, and technology to develop a remediation plan so that there are no issues to VITA and its Customers to perform their day to day operations. The remediation plan will be reviewed with the MSI and approved by VITA before Unisys implements any of the recommendations. The remediation recommendations are prioritized based on criticality to day-to-day operations, impact to VITA users, and level of effort. The remediation activities include the following areas and the evaluation may identify other actions:

- Unisys focuses on limiting the impact of the remediation efforts to the VITA users and will perform these activities within approved change windows.
- Identify End of Life equipment and software. End of Life systems will be identified for the remediation efforts and added to the overall technology plan for the VITA environments due to the duration of the activities or impact to the users (e.g., extended outages, application integration)
- Improve operational and security settings on servers and other IT equipment to align to VITA Rules, and Unisys standards.
- Update Operating Systems to latest service packs or patches. Unisys will also identify Operating Systems, which are out of support and provide recommendations for a separate project to upgrade to a supported version. OS upgrades from older than N-2 to N can introduce operating changes for the VITA applications and must be arranged via the project request process defined within the SMM.
- Improve monitoring of infrastructure or applications. Following the evaluation of the current monitoring systems, Unisys will advise if these improvements can be performed within the current monitoring tools or prioritize these systems to be monitored by the Unisys monitoring suite.
- Prepare the Unisys management and monitoring tools suite – Concurrent with the transition of the current data centers, Unisys will use a separate team to deploy the Unisys tools suite, described in section 2.3 in the QTS and secondary data centers. Implementing tools in these data centers reduces the activities Unisys will need to request of the incumbent and provides flexibility to begin providing services from the new sites once they are connected with CESC and the VITA network. Upon Assumption of Service for the current data centers, Unisys will deploy tools to those environments as well. Unisys will require credentials for all VITA systems to begin deploying the standard agent-less features from the monitoring systems.

The discovery activities will begin prior to the Commencement Date. The discovery will provide the initial data input to the Unisys methodology for learning CoV's key business and IT services. Our methodology includes



five phases (Discovery, Analyze, Strategize, Plan, and Implement). During the Implementation phase, Unisys will perform the activities for the Discovery and Analyze phases to support the development of a technology optimization and remediation plan for the Customers' systems. This methodology focuses on driving incremental improvements at Commencement of Services and advancing optimization to enable Customers to maximize the use of the services proposed in this solution and identify additional services to meet Customers' unique needs. The Strategize and Plan phases are a team effort between Unisys, VITA, its customers, the MSI, and other Suppliers to develop a plan that meets business needs and defines the technical actions for refresh, migration, optimization and extended solutions. VITA, Customer, and stakeholders will review and approve the plan before the Implementation phase begins. **Figure 5.1-1** is an overview of the digital transition methodology and tools used.

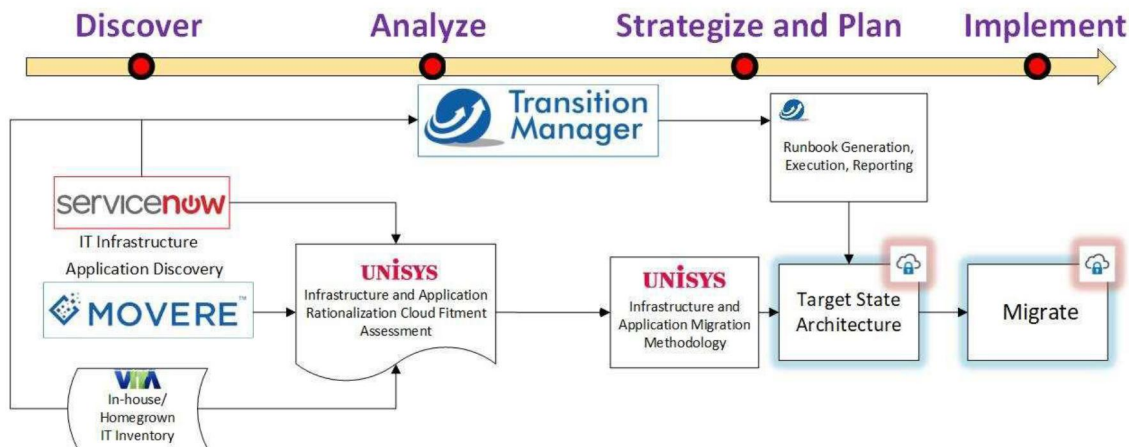


Figure 5.1-1. Digital Transition Methodology.

### Remediation of Current Environments

As discussed in the Directory Services section, Unisys plans to remediate all the AD environments up to [REDACTED]. VITA has stated that they have some remediation projects going like [REDACTED], which Unisys would take over and complete with the help of the MSI and Application owners. A proposed plan will be produced after due diligence to outline which systems will be refreshed or migrated to other platforms so the appropriate costs may be estimated and incorporated into the contract. For example, each Customer Datacenter will be visited to assess what Server and Storage devices will be refreshed and which will not due to age, expected retirement, or early migration to new primary data center at QTS.

## 5.2 Services Evolution

### Service Modernization and Migration

The Unisys Architecture and Service Delivery Management teams evaluate significant changes to existing services and Customer implementations to maintain services to the required service level and avoid business service effects. They advise the application owners on improvements to support adjustments to changing business needs (e.g., increasing capacity or implementing high availability to improve in performance). As new services are developed in the VITA Program and added through the cloud providers, our Architecture and Account Management teams will provide VITA and its customers with recommendations for changes to new options that will improve functionality, availability, performance, or cost.

Unisys applies common standards for hosting services, including verification that hardware includes highly available and redundant components (e.g., power, network, and service modules). These design considerations will reduce the risk of single points of failure affecting service availability during daily operations after CoV's workloads are added to the environment.

During development of new services and new technology evaluations, our Architecture team follows a service design process that assesses the functional and nonfunctional requirements, including those for compliance, security, availability, service levels, redundancy, service continuity, and performance.

Unisys will use this model and integrate these activities with the Service Design, Service Requests, and Architecture governance standards. To support new and updated service definitions, Unisys will perform the following key activities:

- Identify and assess prospective service definition opportunities
- Confirm with VITA and the MSI to pursue or decline service definition activities
- Collect service requirements from requesting Customer stakeholders or define requirements for review with VITA and the MSI
- Develop the service solution proposal, including evaluation of reusing existing services in the VITA Service Catalog and alternatives provided by other vendors and cloud providers
- Review the solution proposal with VITA, the MSI, and Customer stakeholders for approval
- Submit final change requests for Service Catalog modifications
- Initiate a Service Transition project that includes documentation, service validation and testing, and operational signoff before accepting customer workloads.

As new services are developed, plans are defined from the discovery and assessment activities defined in Section 5.1. As Customers' business needs change, Unisys works with the Customers to develop, identify, and plan the right options to optimize each Customer's use of services and migrate to newer technologies, environments, and facilities. As part of these activities, Unisys provide an implementation plan is provided. The plan includes estimates of the migration effort required for Unisys, VITA, and the Customer, including roles; level of effort in hours; and key activities in each phase (e.g., testing, migration, and cutover).

### **Service Currency for Service Evolution**

Maintaining the currency of the VITA environment is crucial to maintaining security, availability and providing the new features released by the vendors. Unisys uses the following workflow to maintain and update systems within the VITA environment. This includes deploying patching, service packs, major and minor releases of software, and new technology. The methodology is further described in *Exhibit 2.3.2 (Solution – Cross Functional) Section 7.6*. Examples of the practices Unisys uses to maintain the currency of systems and perform updates are provided below. Unisys will use this method to support update and upgrade activities identified within the remediation plan, implement projects managed within the technology refresh plan, and independent Service and Project Requests as defined within the SMM.



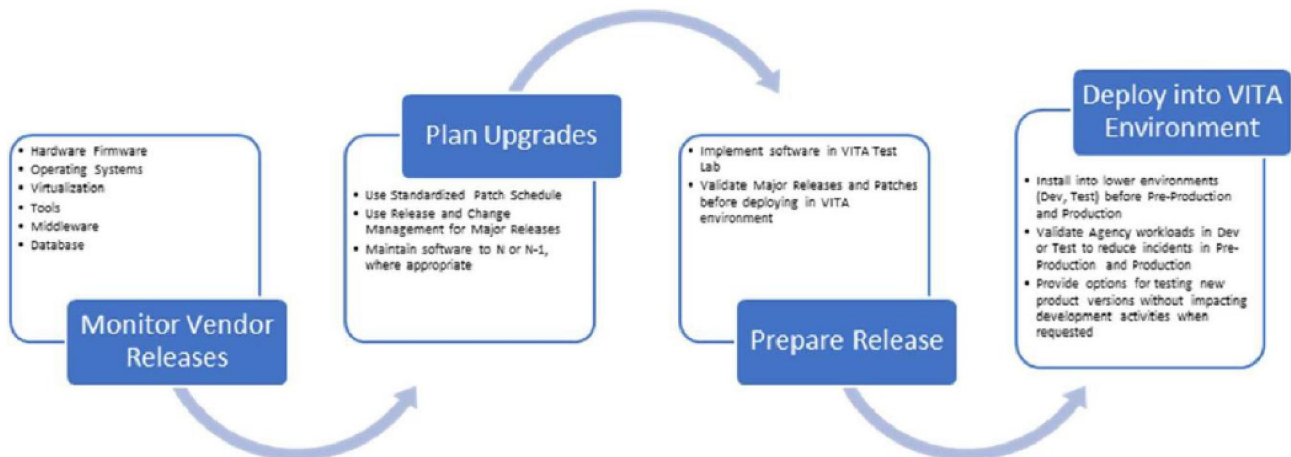


Figure 5.2-1. Software Currency Workflow.

### VMWare Maintenance

Unisys follows VMWare Upgrade and Maintenance practices to maintain the VMWare environment. By using the documented processes from the vendor, Unisys reduces the downtime for VITA and improves the consistency of the deployment.

For VMWare patching and minor updates, Unisys follows the following practice:

1. Set up testing environment, which aligns to target environment.
2. Install updates within the test environment to confirm practices and identify issues, which must be mitigated.
3. Schedule and implement change to update production VMWare management tools such as [REDACTED] if required for update. This activity includes backing up the [REDACTED] and other VMWare management tools and will be performed by switching to the secondary instance during the upgrade of the primary instance.
4. Schedule and implement change to update the Unisys management VMWare environment, if required for update. Performing the change within the separate Unisys management environment provides an additional step to confirm that updates will not impact VITA systems and that the planned activities work correctly.
5. Schedule and implement changes for VITA environment to update VMWare hosts. This is an incremental activity to upgrade an set of VMWare servers within the window without requiring downtime for the VITA systems. This is performed by doing the following activities. If the change window includes more VMWare servers than the available capacity within the current cluster, these tasks will be performed multiple times within the window or managed across separate approved change windows. VITA servers are monitored throughout the change to maintain overall availability and health of the VITA environment. The process is currently described as follows, and may be updated in the SMM.
  - a. At the start of the approved window, Set the scheduled VMWare servers to not receive additional VM guests via [REDACTED]



- b. Use [REDACTED] to move workloads off of VMWare servers targeted for the scheduled change to available servers within the VMWare cluster. If workloads cannot be moved, Unisys will confirm there is a current backup and snapshot of the workloads and communicate with the Customer system owners to arrange the change window to limit impact to the user and business operations.
  - c. Verify all workloads are moved successfully and set the scheduled VMWare servers to not participate in [REDACTED]
  - d. Perform the update on the VMWare servers
  - e. Verify the update was successful
  - f. Set the updated VMWare servers to participate in [REDACTED] and monitor the environment to confirm services are working appropriately.
6. Schedule and implement changes for VITA environment to update VM Guest servers, if needed. This is an incremental activity and will be scheduled following the SMM and require approval of the Customer system owners.
  7. Close changes following the process defined within the SMM.

Maintaining the VMWare environment also requires continuing updates to the N version of the platform for VITA to realize the benefits of the latest features and maintain consistency across the environment.

Upgrading an VMWare cluster and environment to the latest release uses the following practice.

1. Review the VITA VMWare environment using the latest VMWare upgrade documentation and Interoperability Matrix to confirm that the environment can be upgraded. If there are restrictions, Unisys will provide recommendations which may include additional updates, incremental upgrades (e.g. 5.1 to 5.5 before moving to version 6.0), early hardware replacements, or the deployment of a new environment as an initial base either for additional capacity or to use as a foundation to upgrade the remaining environment incrementally based on the technology plan and approved schedule with the MSI and VITA.
2. Set up testing environment, which aligns to target environment including current versions, patches, and service packs.
3. Upgrade the test environment to new major release following VMWare upgrade documentation to confirm practices and identify issues, which must be mitigated.
4. Schedule and implement change to upgrade production VMWare management tools such as [REDACTED] to the new release. VMWare's major releases impact all components and the management tools must be at the latest version before the VMWare servers to maintain visibility and control of the overall environment. This activity includes backing up the [REDACTED] and other VMWare management tools and will be performed by switching to the secondary instance during the upgrade of the primary instance.
5. Schedule and implement change to upgrade Unisys management VMWare environment. Performing the change within the separate Unisys management environment provides an additional step to confirm that updates will not impact VITA systems and that the planned activities work correctly.

6. Schedule and implement changes for VITA environment to update VMWare hosts. This is an incremental activity to upgrade a set of VMWare servers within the window without requiring downtime for the VITA systems. This is performed by doing the following activities. If the change window includes more VMWare servers than the available capacity within the current cluster, these tasks will be performed multiple times within the window or managed across separate approved change windows. VITA servers are monitored throughout the change to maintain overall availability and health of the VITA environment.
  - a. At the start of the approved window, set the scheduled VMWare servers to not receive additional VM guests via [REDACTED]
  - b. Use [REDACTED] to move workloads off of VMWare servers targeted for the scheduled change to available servers within the VMWare cluster. If workloads cannot be moved, Unisys will confirm there is a current backup and snapshot of the workloads and communicate with the Customer system owners, MSI, and VITA to arrange the change window to limit impact to the user and business operations.
  - c. Verify all workloads are moved successfully and set the scheduled VMWare servers to not participate in [REDACTED]
  - d. Perform the upgrade on the VMWare servers.
  - e. Verify the update was successful.
  - f. Set the updated VMWare servers to participate in [REDACTED] and monitor the environment to confirm services are working appropriately.
  - g. Depending on the upgrade guidelines, these upgraded servers may be setup into a new cluster and workloads manually moved via [REDACTED] to the new cluster. This method is used when the upgraded VMWare servers can potentially impact the availability of the current cluster and VITA systems. If this step is required, Unisys will communicate with the Customer system owners, the MSI, and VITA to arrange a change windows to limit the impact to the VITA users and business operations.
7. Schedule and implement changes for VITA environment to update VM Guest servers, if needed. This is an incremental activity and will be scheduled following the SMM and require approval of the Customer system owners as the systems will be rebooted as part of the upgrade process.
8. Close changes following the process defined within the SMM.

### Operating System Upgrades

As VITA systems are identified for Operating System (OS) upgrades, Unisys will perform the upgrade using the following activities after MSI/VITA change control board approves release level and schedule.

### New Deployment

Unisys recommends using a new server instance with the target OS release. This method provides the lowest risk of compatibility issues between the image and the application and avoids legacy configuration or software elements from the previous OS instance and drivers causing performance or availability incidents. This model also enables the Customer system owners to confirm functionality without impacting users.

## Upgrade in Place

Unisys also performs OS upgrades on existing servers. This requires that the OS vendor provides a documented process to perform the upgrade and may require incremental steps and an extended change window to upgrade the OS and enable the Customer system owners to confirm functionality and user testing. Upgrading Operating System in place to the latest release uses the following practice. This practice applies to both physical and virtual server instances.

1. Review the VITA system using the vendor's upgrade documentation and Interoperability Matrix, if available, to confirm that the system can be upgraded. This review requires system owner participation to confirm the application or custom code will be affected by the upgrade. If there are restrictions, Unisys will provide recommendations which may include additional updates, changes in drivers or other components installed on the OS, incremental upgrades (e.g. Windows Server 2003 to Windows Server 2008 before moving to Windows Server 2016), early hardware replacements, or the deployment of a new server based on the technology plan and approved schedule with the MSI and VITA.
2. Set up testing environment, which aligns to target environment including current versions, patches, and service packs.
3. Upgrade the testenvironment to new major release following the vendor's upgrade documentation to confirm practices and identify issues, which must be mitigated.
4. Schedule and implement upgrade for VITA system. Unisys will work with the MSI and Customer system owner to schedule the window as an OS upgrade will require the server to be offline.
  - a. At the start of the approved window, set the monitoring to not notify for the server outage.
  - b. Follow the system runbook or work with the Customer system owner to bring down the application.
  - c. Perform a full backup of the system or take a snapshot to provide a recovery point.
  - d. Perform the OS upgrade on the server.
  - e. Verify the OS update was successful.
  - f. Perform the additional updates required for operations within the VITA environment. OS upgrades can require new drivers, backup and monitoring agents, malware protection and system setting to meet VITA Rules.
  - g. Follow the system runbook or work with the system owner to bring the application on line for testing.
  - h. After the system owner confirms that the application is working as desired, Unisys will perform the activities to bring it back online with monitoring.
5. Close changes following the process defined within the SMM.

## Data Center Services

To replace CESC, Unisys proposes QTS in Richmond. During the Implementation phase, Unisys will develop an implementation plan to integrate the new facilities with the VITA environment after approval from VITA.



Unisys will also develop longer term roadmaps to migrate CESC and Customer environments (as approved by the Customer) to QTS and the cloud. VITA, associated Customers, and the MSI will review and approve migration and implementation plans before following the project and change management activities defined in the SMM.

### Migration to Unisys Data Centers or Cloud Services

Our Migration Methodology is based on the Unisys Data Center Transformation (DCT) Vision. Developed over years of migration experience Unisys has identified overall success factors supporting the DCT Vision:

1. Unisys will support VITA in developing a business case for customers in evaluating a data center migration.
2. Migrations are focused on migrating workloads and infrastructure to reduce complexity and enable a rapid realization of benefits
3. Migrations are collaborative and require input and buy-off from all business, application and infrastructure stakeholders
4. Migrations must seek to avoid a “big-bang only” approach and look to enable manageable (bite-sized) projects.
5. Migrations must be transparent and minimize organizational disruption.
6. The solution must align business drivers with IT initiatives.
7. Acknowledgment and agreement that DCT is a complex journey that requires the robust lifecycle delivery model.

This approach (**Figure 5.2-2**) will serve as the overall process and guiding principle for the migration activity. Within this framework, there are specific tasks and activities defined as part of the Unisys Migration Process.

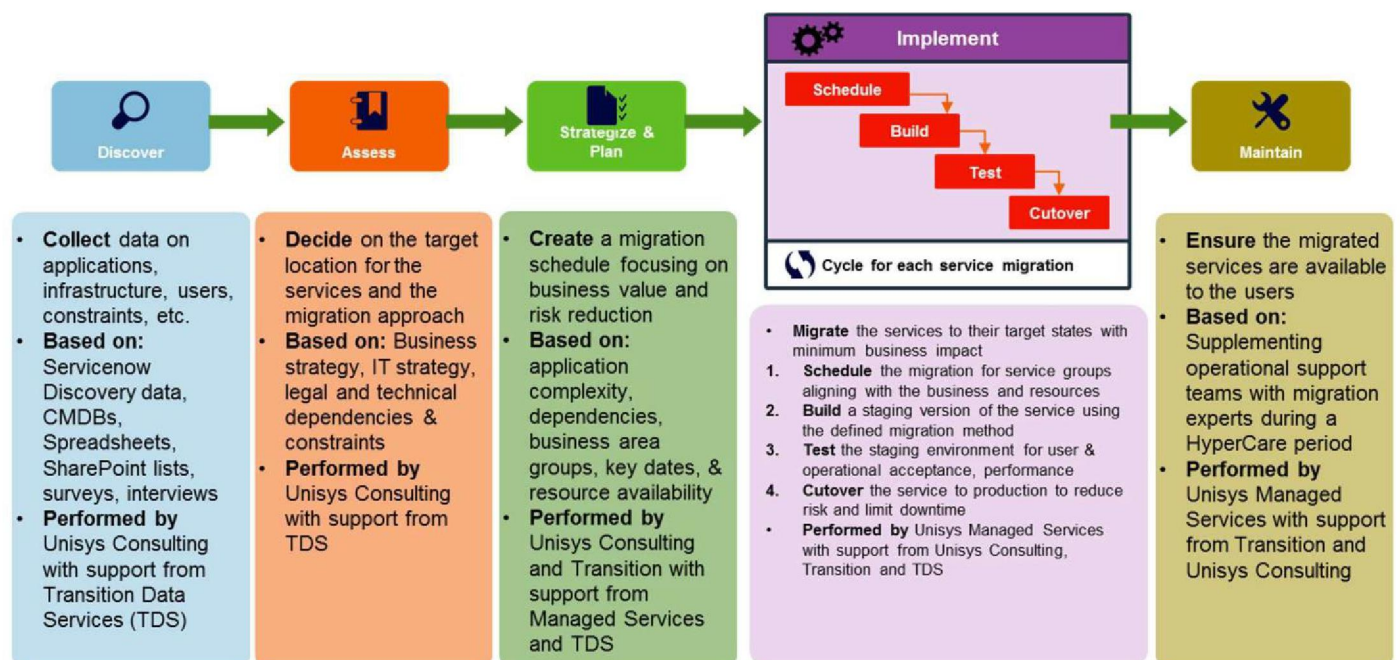


Figure 5.2-2. Data Center Migration Approach.

Key components of the Unisys Migration Process consists of the following phases:

## **1. Discover**

This phase will concentrate on developing a complete understanding of the current application and infrastructure inventory. Unisys will use the physical and virtual server volumes at Primary DC as indicated in Exhibit 4.1 as the baseline for our solution, pricing and discovery efforts for migration activities. Unisys will hold a series of discovery workshops to confirm and validate the applications and servers that are in scope for migration. Once the scope is confirmed Unisys will use a variety of sources to validate information. Sources of discovery include current data sources (spreadsheets, CMDB, service management tools), discovered data [REDACTED] and end user surveys. The combination of data sources will be loaded into a centralized repository contained in the TDS Transition Manager platform described below. This centralized repository provides the Assessment Phase with a validated and up to date data repository that will flow through the remainder of the migration and operations teams. Once the discovered data is captured in the CMDB, Unisys will work collaboratively with the VITA Business Areas to confirm that information required for the Assessment, Planning, and Execution Phases are captured and validated. Based on this information, Unisys will be able to identify the requirements that will be used as inputs to the final overall migration plan.

The Discover Phase will be focused on Business Area and application function. Unisys has established a Discovery timeline and staffing to complete this phase. At the start of the project initiation and planning, the parameters will be validated and adjusted as part of the meeting schedule.

Unisys will establish workshops with each subgroup within the Business Area to focus on the workloads within that area. For example holding workshops for Sales and Marketing – General, Operations – General, and Human Resource for each Business Area. Based on the workload complexity and potential business impact focused workshops within each Business Functional Group will be held.

Discovery will cover the following key areas:

- Validation of the application systems infrastructures using current data from spreadsheets, CMDB and other tools, ITSM tool discovery of application and technical Assets, and web-based end-user surveys
- System and Application Mapping including dependencies and interdependencies
- Identification of requirements such as outage windows, latency, change control process, validation needs, site availability and capacity constraints.

## **2. Assess**

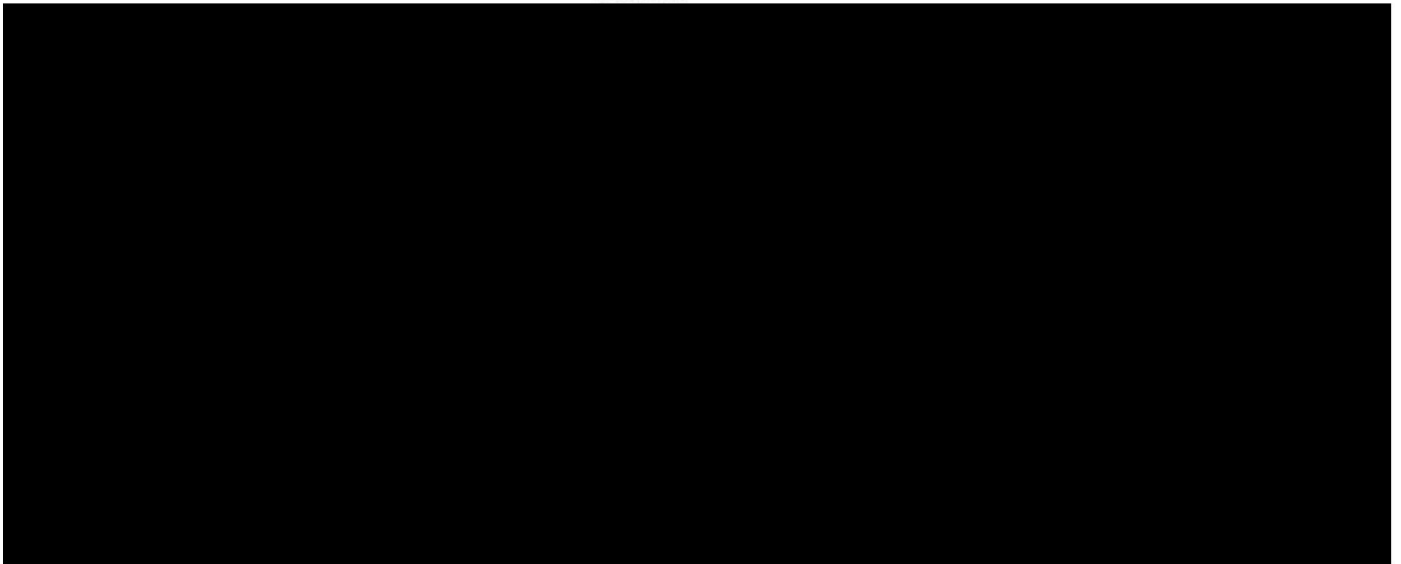
The Assess Phase will, in short, decide where each workload is going and the methods and techniques used to get there. The Assessment concentrates on evaluating the current move group with the application and infrastructure assets and defining the target location for the assets. This activity includes defining the mapping of the existing assets and workloads into the new standardized as a service model as provided by Unisys. In addition to defining the “landing zones” for the current environment, the Assessment plan defines the migration strategy to be used.

Using a defined process that has been agreed with VITA for each workload to be migrated, the Assessment will:

- Identify the target location (QTS Richmond, secondary data center, AWS, Azure, Decommission, or Stay on Premise)

- Decide the migration approach (Over-the-Wire (physical-to-virtual, or virtual-to-virtual), Rebuild, or Lift & Shift)
- Determine service and infrastructure migration complexity
- Socialize and agree on decisions with Application and Business Team to gain support and commitment

Figure 5.2-3 shows the decision paths that can occur for an application being planned to migrate including application refactoring and cloud migration.



**Figure 5.2-3. Application Migration Decision Paths.** *As Each Application Is Reviewed For Migration, Multiple Options Will Be Evaluated With the MSI, VITA, and the Application Owners.*



The common migration approaches used for migrating workloads to the QTS Richmond data center will be:

**Over-the-Wire** – This is also known as V2V or P2V. This option will minimize the duration of the application outage required. For over-the-wire moves, seed hardware is first located in the receiving site and made production ready. A migration approach will be determined based upon platform type to replicate the OS, application and application data onto the new platform at the receiving site. This could include using native tools like VMware or tools like [REDACTED] or use of Storage or Backup replication. An initial copy is executed soon after installation and sync copies are continuously executed leading up to the move event. During the move event, a final sync copy is taken after the application is shut down to verify all data and updates have been received in the new data center. Once the final sync is completed, the hardware in the sending data center is shut down, and the application in the receiving data center is brought up. Once fully started, the Application Support Team will execute the test plan created during the planning process. After a successful test, the application owner will sign-off that it is ready for turnover to the end users. Using this option requires a shorter application outage. This method has low to moderate risk and a lower cost profile when used on assets with less than one year of expected life. As the age of the equipment increases so does the risk but the cost profile decreases due to the expectation of replacing the aging hardware.

**Rebuild with data replication** – In this option, seed hardware (physical or virtual) is installed in the receiving data center, the operating system is installed directly on the hardware, the Application is installed, and then the application's data is copied. Once fully started, the Application Support Team will execute the test plan created during the planning process. After the initial data copy is executed, sync copies of the data are continuously executed leading up to the move event. Once the final sync is completed, the hardware in the sending data center is shut down, and the application in the receiving data center is brought up. Once fully started, the Application Support Team will execute the final test plan created during the planning process. After a successful test, the application owner will sign-off that it is ready for turnover to the end users. This option is used when some transformation activity or a Physical to Physical (P2P) migration is required. Examples could be a new operating system, new application level or database consolidation. This technique is typically used to also upgrade and standardize on operating system and database levels.

**Lift and Shift** – In this option, the current hardware is scheduled for an extended outage window, shutdown, and shipped to the receiving data center. After the equipment is received at the site and acclimated, the system is brought up. Once fully started, the Application Support Team will execute the final test plan created during the planning process. After a successful test, the application owner will sign-off that it is ready for turnover to the end users. This option is used when the data and asset can afford the extended outage, and its usable life and replacement cost is significant. Examples could include new physical assets or equipment maintained for archive or legacy data purposes.

### 3. Strategy & Plan

In the Strategize & Plan Phase, Unisys will determine the initial move group composition, using the decision factors gathered during the Discovery Phase. These logical move groups combine logical application and infrastructure assets that will be included in one migration activity during the Execution Phase, based on key factors such as business groupings, technical affinities, resources, and business need. Based on the defined move groups, a Migration Schedule will be created including the key Go/No-Go gateways. These groups and schedule will be confirmed with all stakeholders to ensure support and participation. This phase will also create the initial workload migration recipes or run-books that contain:

- Technical and Business details of the service needed for migration
- Detailed procedures for application shutdown, server power-off/power-on, and other key technical activities
- Validate back out plans for each migration
- Technical & User Acceptance test plans.

#### **4. Implement**

The steps in the Implement Phase will be repeated for each move group defined in the Migration Schedule. These steps are Schedule, Build, Test, and Cutover.

##### **a. Schedule**

The Schedule provides the final confirmation of the composition of the move group and the migration dates with the required shareholders. The schedule tracks of all follow-on detailed steps, Go/No-Go gates, and final cutover.

##### **b. Build**

The Build for migration begins with the creation, in the target environment, of an initial copy of the workload to be migrated following the specified migration approach. This 'staging' instance is created while the original system remains online to validate that the system is working in the target. This step will span a varied period depending on the migration approach used, and the complexity of the application.

##### **c. Test**

The Test implements the defined technical and user acceptance tests against the staged version of the service. Any specific fixes that are needed for the service to work will be fully documented so that they can be applied during the cutover step.

##### **d. Cutover**

The Cutover is the final move of the service to the target. A final data sync will occur to bring the target version up to date, and then the source version will be taken offline. Final technical and user acceptance tests are performed, and the service is then live in the target data center.

##### **e. Maintain**

Once the service is live in the target environment is now under the new VITA IT Service Management environment with helpdesk and ITSM support. During this Hypercare period, the migration teams are available to support the operations group with any issues that may have arisen as a result of the migration.

## **6.0 Facility Management and Operations**

### **6.1 General Services**

Unisys manages the DC for faults in the environmental systems to avoid incidents that can cause system outages. During the initial assessment, Unisys will identify and test the facility's environmental control systems and tools as well as make recommendations to improve the visibility of the alerts, automate incident notification from existing tools, and enhance information generated by the system.

Additionally, our DC team will monitor the DC equipment, power, and cooling for alarms during each shift. If an alarm is identified, an incident will be created in the MSI's Service Management System to be tracked to resolution.

Unisys' DC management practices include advanced planning for equipment installations to avoid hot spots and facility incidents. Activities for installations are tracked as a service request or change project. Our DC team will coordinate with our facilities building management to perform periodic and emergency environmental systems maintenance in accordance with procedures established in the SMM with a focus on minimizing impact on the Services being provided. This can include conducting repairs of the environment controls (e.g., HVAC, power conditioning, and generators) in coordination with authorized third-party maintenance vendors when required.

Our DC team also works closely with facilities building management to prepare and perform system maintenance and repairs. These activities are coordinated to limit downtime, minimize risk to the compute environment, and avoid potential negative impact on the hosted services and applications. Our DC team will also assist with external DC audits (e.g., federal) to support customers, as directed by VITA.

Our DC team will monitor the DC areas, reviewing camera feeds or other methods to maintain environmental stability, and report issues or recommendation to the facility manager and VITA if necessary. To further improve the security posture, received shipments and inventory coming from the dock of a Unisys owned, leased, or managed DC will be secured in a caged area.

To reduce and limit the exposure to facility-related incidents, our DC support team works closely with VITA, the MSI, the service providers, and third parties to implement the DC policies and procedures. Facility Maintenance procedures are seen as opportunities to practice and test responses to potential equipment failures; these events are reviewed with the onsite team each quarter and discussed to keep the team up to date and prepared in case of an issue. During an incident (e.g., a cabinet fault or an occurrence of a problem), Unisys uses the Service Management tool and Incident Management processes; our team works to resolve the issue as quickly as possible, to include cooling, power issues and fault warning lights with supporting and affected groups.

To enable common activities (e.g., updates in the CMDB, resolving environmental incidents, maintaining the facility, and handling material), our DC Operations team creates run books. The run books describe the activities and workflows that are required to produce consistent results and reduce costs.

Optionally, individual rack monitoring for heat and power is available. Additional equipment or modifications to the rack may be required to enable this capability.

To maintain CESC's appearance, safety, and air quality, Unisys performs ongoing above-the-floor cleaning (at least quarterly) and annual deep cleaning. Office space will be cleaned on a regular basis

Unisys regularly reviews and applies industry trends and standards for changes to the management of the DC, rack management, and environmental support. Unisys will use this information to identify updates to rack configurations and will modify the configurations and product selection to maintain CESC's capabilities while also driving to reduce costs and technical restrictions. This is especially important because of the smaller space requirements and effect of the higher density compute and storage technologies used today for converged platforms and private cloud.



## 6.2 Cabling and Wiring Services

Unisys will manage the cabling and wiring at the primary DCs and secondary data center. This will include procurement, installation and documentation. Unisys will maintain and online Data Center Infrastructure Management (DCIM) platform to track changes.

## 6.3 Security Administration

During the assessment highlighted in Section 6.0, physical security processes, functions, and installations will be confirmed and recommendations identified to align with Unisys standards and industry practices. During the implementation, the procedures for requesting and maintaining access to the DC will be updated in the SMM and be in accordance with VITA Rules.

Access will be restricted to needs-based individuals who will be given access after securing the following credentials:

- Onboarding to the CoV account
- Account Security Training, including VITA Rules; FISMA controls; and HIPAA, CJIS, and IRS-1075 regulations
- DC onboarding
- VITA staff badge with CESC facility and floor access requests
- Manager-approved request to activate authorized zones
- Fingerprint registration session with DC security.

Additional controls or adjustments to the procedures may be required to support specific requirements or regulations for individual Customers. These additional requirements are evaluated as needed and recommendations are made in accordance with the impact on overall operations.

Because CESC hosts VITA and important Customer applications and data, facility access and security will be managed in accordance with VITA policies and Unisys procedures. Working with VITA, the MSI, and facility manager, the access and physical controls are used to limit access to authorized personnel. Parties requiring access to the DC are tracked [REDACTED]

The access logs are reviewed regularly with the security teams. Authorized access is reviewed automatically for privileged access so that user accounts that do not frequently use privileged access are removed from the privileged access groups. Personnel not requiring access are removed from the system [REDACTED]

Security incidents follow the program's security incident reporting process. Information provided by the physical access systems and onsite cameras are supplied to the security teams, VITA, and the MSI as needed to perform the investigation. The physical access systems and onsite cameras will be monitored and maintained to meet Unisys global practices as well as VITA rules and policies to provide a secure facility. Faults and replacements will be tracked and managed [REDACTED]

Security controls also extend to accessing equipment in cabinets to meet unique regulatory requirements. To support respective Customers, cabinets can be locked or optionally set up with additional security controls (e.g.,

cameras, biometric access, or combination locks). The access keys for these cabinets are stored securely, and access is logged.

## 6.4 Biometric Authentication

QTS Richmond has [REDACTED] systems throughout the facility. CESC has [REDACTED]. Unisys will authenticate the systems at the CESC facility and work with VITA and the MSI on updates or changes to those systems.

## 6.5 Cages and Locked Enclosures

Unisys secures racks as part of our standard facility security practices; these keys are stored and restricted to authorized personnel. Access and use of the keys are based on Unisys practices, VITA rules, and the SMM. Security controls extend to accessing equipment in cabinets to meet unique regulatory and security requirements for individual Customers. To support those Customers, cabinets can be locked or optionally set up with additional security controls (e.g., cameras, biometric access, or combination locks). The access keys for these cabinets are stored securely, and access is logged.

## 6.6 Video/Audio Recording

Security incidents follow the VITA Program's security incident reporting process. Information provided by the physical access systems and onsite cameras are provided to the security teams, VITA, and the MSI as needed to perform the investigation. The physical access systems and onsite cameras will be monitored and maintained to meet Unisys global practices as well as VITA rules and policies to provide a secure facility. Faults and replacements will be tracked and managed through [REDACTED].

## 6.7 Access Card Support

Working with VITA, the MSI, and facility managers, access and physical controls are used to limit access to authorized personnel at CESC, QTS, and secondary data centers. Parties requiring access to the DC are tracked [REDACTED].

## 6.8 Facility Environmental Requirements

As a part of VITA Data Center Facility Management, Unisys will manage the CESC facility by providing the skilled resources and processes to support the service's requirements, including the following:

- Create, enhance, and enforce VITA DC facility, security, equipment, policies, standards, documentation, and procedures. As part of the assessment, current policies and standards will be reviewed to identify improvements and updates to align with Unisys and regulatory guidelines.
- Manage the DC space in the CESC facility and provide support and interaction for ongoing maintenance of the facility and related equipment, including service request management, change management, power and space planning, facility spare parts such as patch cables, and cleaning.
- Provide janitorial services for data center and office space.

- Coordinate with VITA, the MSI, and the Suppliers to plan changes, service requests, and IMACs that affect the facility and service operations as part of the overall governance program. Regular and ongoing participation in the change process and program governance will reduce the potential for expedited change requests or service requests for equipment installations, establish a consistent roadmap for power and space modifications, and support ongoing IT service continuity preparedness.
- Provide and maintain an online Data Center Information Management (DCIM) platform to track the facility space use, rack layouts, and power assignments. The DCIM is also integrated with the Configuration Management System (CMS) to support sharing data and providing a comprehensive source of truth. The DCIM tool also provides the data, which when combined with the demand planning for hosted services and each Customer's strategic needs, enables a forward-looking capacity roadmap.
- Provide skilled smart hands support for service providers to assist in IMAC, incident, and change activities that require physical interaction in the equipment or to escort authorized third parties
- Use the available tools to monitor the facility cooling, power, and other environmental factors
- Facilitate onsite tours and support audit-related activities as needed for VITA and supported Customers
- Verify that raised floor areas and aisles affected by work being performed are cleaned thoroughly and returned to the proper state. This could include new rack installations, under-floor work, or activity that can generate waste material. Standard policy is no cardboard boxes, pallets, or anything that can generate particulates (e.g., cushioned chairs) are allowed in the raised floor area. Above the floor, cleaning will take place quarterly; under the floor, cleaning will be performed annually.

During implementation, Unisys will work with the MSI to review and update a DC infrastructure Installation, De-installation, Move, Add, and Change (IDMAC) workflow process in the MSI's ITSM tool system. Unisys will handle the equipment IDMAC requests in tasks and templates from the MSI's ITSM tool. One of the tasks will be to update the CMDB, which would go to the Unisys Asset Manager as well as asset managers for other Service Providers that may be engaged. For Configuration Items (CIs) such as rack location maintenance contracts that cannot be updated through the discovery tool, the asset manager will verify that those CIs are updated. The change cannot be closed until tasks are completed. In accordance with the process, Unisys will work with the MSI to implement the tasks that cannot be closed until the work is completed.

Likewise, equipment is not allowed onto the floor or to be moved or removed without a valid, approved change request. DC personnel will confirm that the changes performed match what is on the change ticket. Again, the person performing these tasks will sign off on them in ITSM tool to indicate that they were completed correctly. This signoff will be documented in the procedures described in Section 6.9. DC personnel will be trained on these procedures and signing off on them to indicate that they understand and will follow them.

Unisys will perform quarterly random spot checks of the CMDB data to verify there are no discrepancies. If discrepancies are found, they are immediately corrected, and the discrepancy's cause is investigated to determine whether it is a one-off error or a subset of data needs further auditing and validation.

As part of the Implementation phase, within the first 4 weeks, Unisys will perform a comprehensive audit of existing CESC procedures to verify that required standard DC procedures are in place. Part of the audit is to verify that the procedures are aligned with VITA and Unisys standards and policies. The policies will be compared with the approximately 70 Unisys standard SSAE 16, ISO 27001, ISO 9000/20000 certified procedures in place at Unisys managed DCs. If procedures are missing, incomplete, or lacking, Unisys will



implement our standard procedures, again confirming that they meet or exceed VITA policies and requirements.

## 6.9 Personnel and Visitor Monitoring

Employees who require access to the DC will submit an online request. Unisys DCs use the [REDACTED] system, for controlling facility access, which [REDACTED] allows us to define a workflow with the appropriate management approvals. If VITA's [REDACTED] system does not have the equivalent capability, Unisys will work with the MSI to develop a Service Request workflow [REDACTED]. In that workflow, access must be approved [REDACTED]. Access must be preapproved through the workflow system [REDACTED]. If the preapproval is not processed, access is revoked. For Customers that have additional restricted areas in the DC (e.g., cages or locked cabinets), Unisys will work with VITA and its customers to implement an access policy that would meet their requirements (or develop a policy if none exists but is required). [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Once these requirements are met, the employee signs a document confirming that he or she is aware of work rules and safety features.

Because the CESC, QTS, and secondary data centers host VITA and important Customer applications and data, the facility access and security are managed in accordance with VITA policies, the SMM, and Unisys procedures. Working with VITA, the MSI, and facility managers, access, and physical controls are used to limit access to authorized personnel. Parties requiring access to the DC are tracked [REDACTED]. [REDACTED] The access logs are reviewed regularly with the security teams. Authorized access is reviewed automatically for privileged access so that user accounts that do not frequently use privileged access are removed from the privileged access groups. Personnel not requiring access are removed from the system [REDACTED].

Security incidents follow the program's security incident reporting process. Information provided by the physical access systems and onsite cameras are supplied to the security teams, VITA, and the MSI as needed to perform the investigation. The physical access systems and onsite cameras will be monitored and maintained to meet Unisys global practices and VITA rules and policies to provide a secure facility. Faults and replacements will be tracked and managed through the MSI ITSM tool and the Security Incident Management process.

## 6.10 Remote Management

Remote management of physical areas will follow the documented practices for the CESC DC facility to monitor for any unauthorized access and that any third party connections to any environmental management systems are managed in accordance to VITA Rules and the SMM.

## 7.0 Server and Platform Services

During the Implementation phase, Unisys performs discovery, shadowing, and knowledge transfer activities to establish the foundation to assume service operations duties at Commencement of Services. These activities

align Unisys practices with current functions and enable us to assume control and responsibility of services immediately.

Upon Commencement of Services, Unisys' managed server service support model will manage the Managed Environment, including services hosted at the VITA CESC facility, Unisys hosting facility at QTS Richmond, [REDACTED], and VITA-designated remote locations. Unisys provides the security and management support throughout the life cycle of servers, server appliances, and platform-specific infrastructure from installation to decommissioning.

Unisys managed server support is designed with security at its core and applies related controls in the support model. Our CEs undergo security training for engagement resources and advanced security certification of team leads across delivery tower functions. The required training for staff to support VITA and our other clients is above the industry average, updated yearly, and tracked through our eLearning system.

Unisys approaches server management as outlined in *Exhibit 3.1 (Service Level Matrix)*, which focus on server availability, hours of support, and customer environment. These tiers provide VITA with flexibility to meet specific operational needs while providing a consistent, secure, and well-managed environment. The server availability is based on individual servers and does not supersede SLAs for availability of application environments. These tiers also integrate with the proposed RTOs and RPOs for business continuity and DR to maintain services and operations once an Customer's application environment is moved to a DR state. During the Implementation phase, Unisys will work with VITA to define additional components of the tiers (e.g., privileged access restrictions and standardized reboot schedules that can be added to the service tier description or documented in the system's run books).

## 7.1 Common Platform Services

As described in Sections 2.3 and 7.0, Unisys assumes service operations at Commencement of Services for console operations, monitoring, and management for servers, storage, application services, and related network infrastructure.

Unisys provided tools and integration with the MSI dashboard and reporting systems enables visibility and access to monitoring data and automated system generated ticketing. Upon request, Unisys also provides role-based access and use monitoring and automation tools and assists Customers with enabling their specific monitoring tools. Unisys will encourage using common tools to reduce load on the environment, improve time to resolution, and reduce overall program cost. Unisys will work with VITA, its customers, and the MSI to optimize and improve services to meet continuing and new needs as well as find additional synergies in the environment to reduce complexity or enhance service capabilities.

### Application Packaging

Unisys provides application packaging services to support the deployment and promotion of applications in VITA's Citrix server environment. Requests for application packaging, including application patches, will use the Service Request, Change Management, and Release Management processes described in *Exhibit 2.3.1 (Solution – Cross Functional)* and *Exhibit 2.2 (Description of Services – Cross Functional)*. Additionally, application packaging follows the Release Management process to reduce incidents and service outages caused by packaging or scripting errors and maintain an open flow of communications among application owners, VITA, the MSI, and Unisys. These application updates and packages will be tracked in the MSI ITSM system with completion (or failure) status details.

Unisys uses application packaging functions in the CMP tools and product/platform specific tools (such as [REDACTED]) to automate the deployment of application packages. The ability to use the most appropriate tool to release the packages reduces the time for deployment while maintaining the proper controls to respond to failures and roll back the environment. Packaging and deployment failures will be managed using the Incident Management and Problem Management processes to maintain the end-to-end life cycle of the requests.

Unisys will support the current Netscalers and implemented functionality.

### Server Administration

Unisys performs server administration services, including the various tasks required to maintain the operational configuration for individual servers, groups or clusters of servers, and server appliances. Using run books (described in Section 2.3) and service requests, Unisys provides deployment, installation, maintenance, and monitoring for server functions, including the following highlights based on VITA security, operations standards, and the SMM. Servers are configured according to approved and documented baseline server configurations, and such baseline configurations are monitored and maintained.

- System Configurations (naming conventions, IP tables and name file configurations, and file systems)
- Directory and Structure Management (adding and deleting group permissions and file shares; amending security access right and attributes to data shares, directories, and data files; file and directory cleanup after user removal; review and resolution of disk fragmentation and server quota levels)
- Local User Privilege Management (local user creation, permission definition, and removal; server integration with VITA-approved directory services (e.g., LDAP, Okta, federated directories); password reset and revocation)



- Print Server Management (managing and resolving server-based print spool management).

As described in Section 2.3, Unisys monitors server environments with event monitoring to identify, respond, and resolve incidents based on performance of the infrastructure and supported applications. Working with VITA, the MSI, and other Suppliers, Unisys will provide ongoing support to resolve complex issues that span Suppliers and organization management domains.

Unisys uses the reporting functionality from the MSI and our ODS, highlighted in Section 2.9, to review for trends and problems to maintain and improve overall operations for VITA’s environment. Reports on utilization and capacity trends are provided and performed as described in Section 2.7.

## 7.2 Server Services

Unisys’ Managed Compute Services team works 24x7 with VITA and the MSI to develop standards, controls, program-focused and Customer-specific operational documentation, and maintenance plans for the server configurations, including directory settings and structures and naming standards. It is crucial for the standards to be consistent across the environment to reduce the time to implement and support automation. Unisys also builds these standards and controls into the server provisioning and automation functions.

Unisys assumes service operations at Commencement of Services for console operations, monitoring, and management for servers and platform covering the hardware, hypervisor, operating system, and tools.

The Digital Innovation journey to the FMO will focus on optimization program that will bring an agile, standardized, rightsized FMO virtualized private cloud-based compute environment to VITA in an “as a Service” model. Working with the MSI, Unisys will create a standard service catalog to cater to VITA and its customers for the enterprise compute environment. FMO will be built on 95 percent [REDACTED] [REDACTED] virtualization and the Unisys CMP for orchestration and automation of services.

Unisys will rely on VITA to perform the following activities to support Server services:

- Provide appropriate maintenance windows to support upgrades, patching and remediation activities

### 7.2.1 General

Unisys uses a common management and operations methodology across the platforms at VITA, including cloud IaaS, x86-based servers running Windows and Linux; a midrange UNIX system running AIX, Solaris, and HP-UX; and server appliances. Service tiers are noted in Section 7.0. Unisys Managed Compute Services provide the VITA IT environment with the following standard services. Unisys support teams also collaborate and work with VITA, the MSI, and other Suppliers to improve the efficiency and standardization of processes across the environment. Unisys will work with the MSS to provide access to all log sources within the SSDC environments.

<ul style="list-style-type: none"> <li>• Monitoring and Availability (see Section 2.3)</li> </ul>	<ul style="list-style-type: none"> <li>• Break/Fix Support and Incident Resolution (see Sections 2.3, 2.6, and 2.8)</li> </ul>
<ul style="list-style-type: none"> <li>• Capacity and Performance Management (see Section 2.7)</li> </ul>	<ul style="list-style-type: none"> <li>• Anti-Virus (AV) Management for Servers</li> </ul>
<ul style="list-style-type: none"> <li>• Operating System and Hypervisor administration (see sections 2.3, 2.4, and 2.6)</li> </ul>	<ul style="list-style-type: none"> <li>• System Documentation and Run Book Management (see section 2.6)</li> </ul>

<ul style="list-style-type: none"> <li>• Server Provisioning and Deprovisioning using automated and manual procedures including configuring and managing routing administrative functions</li> </ul>	<ul style="list-style-type: none"> <li>• ITIL process adoption to bring in maturity and standardization</li> </ul>
<ul style="list-style-type: none"> <li>• Hypervisor, Operating System, and Middleware Patching and Hardware Firmware Upgrade (see Section 2.4)</li> </ul>	<ul style="list-style-type: none"> <li>• Automation of standardized and recurring tasks using tools and scripting</li> </ul>
<ul style="list-style-type: none"> <li>• Software distribution during server provisioning and as part of the release management process</li> </ul>	<ul style="list-style-type: none"> <li>• Maintain desired state configurations and privileges are tracked using automation and regular audits.</li> </ul>

## 7.2.2 x86 based commodity Servers

As described in Section 2.3, Unisys assumes service operations at Commencement of Services for console operations, monitoring, and management for servers, platform, storage and related network infrastructure. Unisys will continue to manage the CMO traditional virtual infrastructure leveraging the existing [REDACTED] management tool until the migration of last workload from CMO to FMO.

The Unisys solution will offer the service in an “as a Service” model with standardized service catalog that is carefully designed to replace the current CMO environment. The FMO will offer vendor supportable operating system (OS) revisions in the platform across x86 and non-x86 systems. Operating Systems that are older than N-2 will require a project to upgrade to current version. The virtualized private cloud platform offers compute instances based upon approved blueprints for Windows and Linux platforms. These will follow similar standard compute sizes from Public cloud providers. VITA and Unisys will agree on the blueprint and compute sizes. As a fallback option for workload that requires a proprietary solution, the Unisys Service Catalog will offer standard-sized physical compute solutions. Unisys will work with Customers and VITA to recommend custom solutions or update the standard configurations to meet unique or new requirements. These solution support different availability tiers to meet diverse business requirements. Tier 2 will offer a High Availability (HA) virtualized environment. Although the Physical Services tier requires careful planning and designing of the platform where HA and DR are required, it cannot take advantage of the virtualized FMO Tier 2 for an application or other reasons on case-by-case scenario.

Unisys understands the requirement for VITA’s need for direct-attached storage on a physical server platform; therefore, our service catalog will include the Dell Direct Attach Storage (DAS) solution with small, medium, and large capacity to meet custom storage requirements when a SAN or Network Attached Storage (NAS) is not recommended.

Unisys will work with VITA application and other stakeholders as necessary to understand the CMO and business requirements and come up with a migration plan for each identified workload to the FMO in phases with about 25 percent of workload to FMO.

### Enclave and Containerization

Unisys includes enclave and containerization management and services for application-centric and infrastructure-centric containerization as a component of the server and platform management services. Although infrastructure-centric containerization on the Red Hat Enterprise Linux (RHEL) platform, including OpenShift, provides the core containerized solution, application-centric containerizations require assessment of VITA applications to understand the remediation requirements to enable Customers’ use of the technology



and maximize the value of containerization for CoV. This will also help in understanding the need for vendor-specific commercial containerization solutions (e.g., Docker) for VITA's environment.

Unisys' approach to container application platforms enables organizations to build, develop, and deploy easily and quickly in nearly any public or private cloud infrastructure. The following concepts apply by default to Unisys container services and are at the core of what makes containers secure on the platform:

- Linux namespaces enable creating an abstraction of a particular global system resource that can be used simultaneously
- Security Enhanced Linux provides an additional layer of security to keep containers isolated from each other and from the host
- CGroups (control groups) prevent containers on the same host from affecting each other. They also limit, account for, and isolate the resource usage (CPU, memory, disk I/O, network, etc.) of a collection of processes.
- Secure computing mode (seccomp) profiles can be associated with a container to restrict available system calls.

### Application Refactoring

Application refactoring is the restructuring existing code to improve its performance, readability, portability, user experience, or code adherence without changing the code's intended functionality.

Applications are refactored mainly to take advantage of a cloud provider's various native services. When migrating applications to the cloud, Unisys recommends the following two-pronged approach:

- **Lift-and-shift**, in which the application is ported directly with minimal code modifications. Applications that use a well-defined architecture in which the data is paired with the application logic and the data is difficult to separate are ideal for lift-and-shift.
- **Refactoring**, in which Unisys customizes the application to run on a cloud platform will be a unique process for each application; Unisys will scope and price it for VITA as appropriate candidates are identified. Poorly designed business applications have significant risk when they are lifted and shifted to the cloud. Unisys introduces the concept of containerization, using [REDACTED].

### Private Cloud

Unisys' proposed server solution can extend the traditional virtual commodity server platform's functions to meet the requirements for the CoV Private Cloud. Unisys proposes a Service Catalog-driven Private Cloud solution as part of our FMO solution. VITA and its customer teams will access the Unisys Server Service from a Service Catalog that Unisys will build with the MSI to integrate with the underlying hardware and compute infrastructure. The pricing includes the hardware, software, maintenance, tools and support services and varies depending on the storage technology as that is the main driver of the price. Unisys will collaborate with the MSI to assist VITA and its customers in selecting and consuming the CoV Private Cloud vs. traditional physical or virtual servers. This would be in accordance with the defined SMM/Procedures Manual. To enable quick and inexpensive proofs of concept to VITA and its customers, our private cloud solution brings in flexibility, scalability, and agility to our solution for faster provisioning and deprovisioning.

The Private Cloud Service is integrated with the MSI Service Catalog and Unisys CMP to enable on-demand self-service, secure network access in accordance with VITA security controls, resource pooling, elasticity in



the private cloud, and support for expanding and moving workloads to the public cloud, and transparency of service operations. VITA and its customers can unilaterally provision computing capabilities (e.g., server, network, and storage) as needed automatically without requiring human interaction with Unisys. To make this possible, Unisys will have a scalable and agile infrastructure environment in place to handle VITA and its customers' requests automatically. The infrastructure to be provisioned will be virtualized so that different Customers can use the same pooled hardware.

CMP captures sufficient information to support audit and compliance in the broad audit categories of financial/compliance, performance associated with SLAs, security incident and management, and adherence to VITA policies that provide threshold metrics such as requirements for 100 percent staff with security clearances and 100 percent achievement of annual training.

### 7.2.3 UNIX Based Servers

Unisys Managed Server Services provide common management and operations methodology across the platforms at VITA, including IaaS, x86-based servers, and UNIX server appliances. As described in Section 2.3, Unisys assumes service operations at Commencement of Services for console operations, monitoring, and management for servers, platform, storage, and related network infrastructure. Our UNIX Server technical team will provide support for HA configuration, multipath I/O configuration, and DR services in accordance with the requirement. Unisys will create collaborative teamwork with VITA, the MSI, and other third-party services where necessary to provide proactive managed services. Unisys will provide consultancy and architecture level guidelines and required artifacts to provide rightsizing for UNIX and its platform services in a timely way.

Our implementation of digital innovation will focus on optimization that will bring agile, standardized, rightsized FMO virtualized private cloud-based compute environment to VITA in an "as a Service" model. FMO will be a virtualized x86 RHEL platform to host non-x86 CMO workloads. This will include the existing IBM WebSphere Application Server (WAS) environment. Unisys understands that non-x86 platform workloads will be needed because of an application's dependencies or other constraints. To address this workload requirement, Unisys proposes IBM and Sun Solaris vendor-specific UNIX hardware platforms in the FMO. However, Unisys will assess this requirement further as part of due diligence. Apart from vendor-proprietary, non-x86 hardware, Unisys also considers the need for an x86 RHEL physical hardware-based solution where necessary; this requirement will require us to assess the workload further.

## 7.3 Database Services

Unisys' Managed Database as a Service (DBaaS) will support and include change plans in the size of databases that result from business growth, project implementation based on information supplied by VITA and its customers, and review plans with the MSI, VITA, and ITISP Governance regularly for comments and approval. Key features of DBaaS include monitoring and preventing out-of-capacity situations proactively with dataset or table space capacity events and full log files. Unisys will develop, document, and maintain physical Database Support and management standards and procedures based on industry best practices as well as VITA and its customers' needs.

During the Implementation phase, Unisys will create a DBA support document listing contact information (phone and email) for our SMEs as well as Customer DBA contacts. **Figure 7.3-1** is our standard RACI matrix for

database support. During implementation, Unisys will tailor this matrix to meet VITA and its customers' requirements. Unisys do not view RACI matrices as one size must fit all.

Task/Function	Description	Unisys	VITA
Database Installation	i. Install, configure, and maintain database software	AR	IC
	ii. Perform, document, and maintain patches to database software following agreed schedules and approved RFCs		
	iii. Create new databases		
	iv. Provide Information required to create a new Database	I	AR
	v. Full Testing Life Cycle after Patching and User Acceptance		
	vi. Provide Licenses Required for New Database Installations		
Database Backups	vii. Define Versions and Packages that need to be Installed in each new provisioning		
	i. Manage DB Backups – Verify & Resolve Backup Errors	AR	IC
	ii. Restore & Recover databases from backups limited to the ones required to restore services availability (recover from incident, from crashes, etc.)		
	iii. Manage DB Exports – Verify & Resolve Backup Errors		
	iv. Configure and Schedule New DB Exports as per Client Agreed Policies		
	v. Propose Improvements on Backups		
Database Security	vi. Define Backup Policies	I	AR
	vii. Approve Backup Recommendations		
	viii. Provide required resources for Backup Improvement Recommendations		
	i. Enable Database Audit according to the Client Request/Policies	AR	IC
	ii. Execute Password changes as per client Request		
	iii. Create/Modify Agreed Clients Policies		
	iv. Create Files as requested by Client		
	v. Create Files as requested by Client		
	vi. Create Files as requested by Client		

Figure 7.3-1. Unisys Standard RACI for Database Support.

Unisys will provide a value-add database cloning platform that also provides a fast and consistent data masking capability that provides a consistent but anonymous version of personally identifiable information in the production database. Our integrated platform builds on the technology provided by our partner Delphix to deliver DBaaS to support common application requests through automation.

Unisys will work with the MSI to offer application developers a portal of database platform self-service tools to enable roll-forward and rollback quickly and efficiently to help expedite the application development process.

Unisys enables Tier 1 SAN storage to support primary production databases with advanced cloning and masking services. Unlike current processes of copying databases to alternate locations for use by test and development staff, our DBaaS provides a nearly instant snap of the production database. The snap clone is then examined to insert a masked value over personally identifiable information. Test and development staff can mount as many separate copies of the snap while our DBaaS tracks the changed blocks that occur as each developer manipulates his or her virtual copy of the database. This approach provides rapid access to copies of databases with masked anonymous data and dramatically reduces the storage used in a traditional development, testing, quality assurance, and production cycle for database development.

Our VITA application team will access the Unisys DBaaS platform from a Service Catalog that Unisys will build with the MSI to integrate with the underlying hardware and compute infrastructure. Our database service staff will provide migration services for existing databases to bring these under DBaaS platform management. Our DBaaS will manage MS SQL Server, Oracle, Oracle RAC Database platforms, and AWS database formats, including management for logical and physical database activities.

Unisys will also use the tool's cloning capabilities to speed migration of databases to public cloud implementations. VITA customer staff can combine the cloning and masking to remove the security risk of testing database developments on a burstable public cloud infrastructure and remove the costs and time associated with building on-premise infrastructure.

The Unisys built Delphix technology delivers automation to support these common database operations.

## **7.4 Appliance Services**

Appliance platforms provide options for supporting specific application and functionality needs in many applications. Unisys services enable, provision, and manage appliances based on Customer's needs and technical requirements. If the appliance requires OS administration, the Unisys server services already described are used to maintain system availability and currency. Unisys also provides support for appliance-preinstalled software and applications from our rate card and new solution development as needed for Customers.

### **7.4.1 Physical Appliance Services**

The Unisys Data Center Smart Hands Service installs physical appliances, including network and power, and works with our System Support team to configure the appliance as requested by Customer or appliance vendor. Unisys set appliances up for monitoring and alerts for maintaining availability. Physical information is recorded in the DCIM and CMDB to support ongoing operations and service requests, including reboots and shutdowns.

### **7.4.2 Virtual Appliance Services**

Virtual appliances can reside in the virtualization environment or cloud services. To enable a flexible implementation for a Customer, Unisys uses the virtual appliance's image with our CMP automation services to provision, configure, monitor, and maintain the system. Additional automation from service requests can enable backups, replication, and updates.

## **7.5 Other Platform Services**

Unisys services for application service management, which include virtual desktop, application virtualization, and middleware, enables VITA and its customers to focus on their business needs while receiving services designed to meet VITA's security and functionality requirements.

### **7.5.1 Virtual Applications and Utility Applications**

Unisys uses a persona categorization approach to identify use cases for business applications that are best served to VITA's client base from a Citrix or virtual environment, taking the appropriate end point devices into account. Unisys will plan, build, and operate multiple vendor application and desktop virtualization platforms across a diverse set of industries and will bring ITIL v3 best practices and our experience to develop VITA's operational processes. Unisys focuses on Security Identity Access Management, self-service integration with ITSM tool, service catalogs, workflows, orchestration, and automation as a means to reduce the total cost of ownership and complexity. Unisys planned, built, and managed large-scale public, private, and hybrid cloud solutions. Our focus and experience with virtualization platforms, vendor strategies, third-party tools, and platform features are key to our ability to providing a more robust, efficient, and reliable solution for VITA and its customers.

Standard Services provided as part of Unisys solution are as follows:



- Packaging, configuring, upgrading, distributing, retiring, and installing hosted business applications
- Managing the Business Application User Acceptance Testing (UAT) process
- Installing, configuring, testing, retiring, patching, and monitoring the Citrix platform
- User entitlement to applications processes
- Coordinating dependencies of the Citrix environment (DMZ, AD, Enterprise Directory)
- Managing Citrix Policies
- Managing release and update processes
- Problem Management process for Citrix environments and client dependencies (configuration offirewalls, thin clients, and Independent Computing Architecture receivers)
- Managing documentation and repositories for:
  - Platform and application change processes
  - Citrix Policies
  - Configuration of business applications
  - Troubleshooting firewalls and connectivity
  - Design and maintenance processes for Citrix Platform and Business Application (UAT) Test environments.

Unisys must assess the Citrix Server environment, which hosts VITA business users' applications (XenApp), to understand the number of Citrix servers, roles, and farms. The complexity will also vary by the presence of cross-site infrastructure. Additionally, the type and number of applications with users and geodistribution will influence our solution. To deliver the Citrix platform service requested as part of Section 7.5.1, Unisys will leverage current toolsets.

## 7.5.2 Middleware Services

### Middleware Platform Management Services

#### Option 1 – Collaborative VITA Managed Middleware - VITA owns hardware and provides Middleware software support with Unisys providing AIX platform support.

Unisys proposed solution to VITA is to provide “Collaborative VITA Managed Middleware” services described in the below table. Unisys infrastructure team and VITA middleware administrators to collaborate and develop an integrated maintenance schedule to provide regular and critical maintenance activities, such as security patches or bug fixes are addressed in a timely manner with minimal disruption of services. Support for this option is included in the support for the AIX platform.

#### Collaborative VITA Managed Middleware – Option# 1

1. Provide Support for the Collaborative Middleware Infrastructure (i.e., [REDACTED] or higher).
2. Refresh of the Power 7 infrastructure will be covered by HSC and will be sized to take advantage of improved hardware choices.
3. Provision and Support shared Process pools per VITA requirements.
4. Provide technical Support for Middleware Infrastructure.
5. Perform operational activities and interface with other teams and Third Party Suppliers, including: Monitor, Installation, Configuration, provisioning (e.g., Software, LPARS, Network connectivity, SAN, facility space), Update, Patch, backup and recovery.

6. Assume and maintain current Middleware Software licenses, which Support these Services as requested by VITA.

**Figure 7.5.2-1. Collaborative VITA Managed Middleware.**

## 8.0 Storage Services

Unisys Managed Storage Services is designed to provide a 24x7 Single Point of Contact (SPOC) for storage management requirements with lower OpEx costs and improved service quality. Unisys understands VITA's complex storage environments and provides a wide range of services to maintain and support the storage environment at CESC and Customer sites during CMO and at the target Unisys DCs during FMO.

Our solution comprises storage and backup devices from industry leaders (e.g., Dell EMC and Brocade). The environment requires multiple levels of speed, redundancy, scalability, availability, and security.

As a part of FMO, to maintain high I/O performance requirements for applications and databases, QoS can also be turned on to help obtain the highest benefit from the hybrid design with flash drives, whereas general file systems can often live on SAS or NL-SAS drives. Synchronous replication exists in the environment for higher Tier 1 Services, considering VITA's requirement for an Active/Active storage solution. Unisys' storage offering can provide secure and encrypted storage replication that is enabled for service levels and tiers. Expected storage tiers with availability are considered in the solution that is delivered from single or dual DCs, considering that distributed Customers' business center and site data will be stored at centralized sites and replicated to the DR.

Unisys understand the business needs and protection level of applications, and databases and will work with Application and DBA's from Customers in collaborating with VITA and MSI to provision storage with optimal performance capabilities.

Unisys solution is based on different storage classes have been defined and will be provided by different storage technologies, integrated to the VITA's infrastructure Service. The storage tiers are defined in Exhibit 4.2 (Resource Unit Definitions).

### 8.1 Storage Management

The Unisys Managed Storage Service will provide remote 24x7 management of VITA's storage environment. The CIs that make up the storage environment (e.g., storage array, SAN switches, and NAS filers) will be monitored and kept available in accordance with the SLAs. **Figure 8.1-1** provides the mapping of RFS requirements for storage services to Unisys solution compliance and approach. Unisys' Storage Management responsibilities include levels and types of storage (e.g., NAS, SAN, and locally attached Server Storage DASD).

During implementation, Unisys will create a storage support document that lists contact information (phone and email) for our SMEs and the Customer contacts. Our Storage Services staff will provide migration services

for existing storage devices residing at CESC and in VITA Customers locations to bring them under Unisys Storage Service management. Our Storage Service will manage current and future on-premise storage landscape and Public Cloud Storage. Refer to Section 2.4, Implementation Plan for information on how Unisys will manage CMO and strategize the migration of workloads to FMO.



Figure 8.1-1. Storage Target Landscape (FMO).

**Management, Monitoring, and Health Checks** – Storage environments typically provide redundant components to achieve high availability levels. Appropriate monitoring and alerting as well as regular health checks are key to confirm that redundancy levels are restored before they affect performance and availability.

Figure 8.1-2 identifies the service Unisys will provide for Storage Management.



Unisys follows vendor-specific, best practices-based monitoring of key components and metrics in storage infrastructure. Following are the key activities:

- Review array, SAN alerts, and performance alerts; take required actions
- Fine-tune the alert thresholds
- Check dial-home status
- Administer system (operating system and hardware)
- Check for failures in the array and the SAN
- Check for local replication jobs success and failures
- Check for remote replication status
- Evaluate, implement, maintain, manage, and monitor disk, SAN, and NAS environments

**Provisioning/Reclamation** – Unisys follows a well-defined process for addressing new storage requirements from simple NAS file extension to the complex SAN requests involving local/remote replication. To perform these activities, Unisys will evaluate the performance requirements and analyze the current workload on storage systems (see Sections 2.3 and 2.6). Key activities are as follows:

- Review storage requests
- Deallocate storage and perform required cleanup
- Provision block/file storage
- Add new servers to existing SAN infrastructure

**Proactive Performance Management** – Performance Management is done monthly by analyzing various metrics to provide customers and Unisys management with a detailed view about the storage array performance.

Unisys will provide recommendation and migration plans for moving data across storage arrays NS tiers for better performance, if required. This proactive performance management approach helps to avoid future performance issues. Key activities are as follows:

- Provide a periodic general array performance analysis report
- Understand the workload profile
- Create workload performance baseline
- Analyze workload changes (normal growth, additions, anomalies)
- Perform storage and SAN tuning
- Provide data for planning of additional workloads
- Benchmark IOPS capability of each tier and pool
- Recommend tiers and pools for the new workload
- Provide recommendations for preventing performance issues
- Provide standard and ad hoc capacity reports

**Software/Firmware Upgrades** – A Unisys SME will perform the required analysis and work with the OEM vendor to identify the software/firmware upgrade requirement. Key activities are as follows:

- Analyze technical advisories and alerts from the OEM
- Assess and validate upgrade requirements to target the software/firmware level
- Perform pre-upgrade checks and validation
- Plan upgrades
- Create a change record
- Coordinate with other support teams
- Perform upgrade tasks
- Perform post-upgrade checks.

**Break/Fix Support and Incident Resolution** – This involves coordination with DC facilities team and the OEM vendor for hardware replacement activities. Key activities are as follows:

- Analyze the hardware failure alert
- Upload the diagnostics log
- Coordinate with the OEM and DC Facilities team for hardware replacement
- Log a case with the OEM vendor
- Create a change record for hardware replacement
- Verify the component's health after successful replacement.

**Local and Remote Data Replication Management for DR** – This involves operations support for the local or in-system replication and remote replication for disaster recovery purpose. Key activities are as follows:

- Troubleshoot storage replication issues
- Configure new replication groups in the existing arrays
- Add new devices in the existing replication groups
- Support data recovery using a local snapshot or a clone
- Support DR exercises.

**Documentation** – Maintaining up-to-date documentation is important and serves as a ready reference for troubleshooting issues and for planning activities. This involves maintaining an updated operational support document with contact details for various support teams and managed devices information.

**Figure 8.1-2. Storage Services.**

### 8.1.1 External Storage Media Management

Although Unisys understands that CoV does not plan to expand its use of tape storage and is working to migrate archival and backup libraries to storage, Unisys will maintain the current capabilities during CMO.

Unisys will perform operational responsibilities for external storage media, including offsite media storage as well as onsite and offsite management functions, for operations and administration of external storage media libraries. This specifically includes the following tasks:

- Mount or initialize external storage media retrieved on site and off site
- Dispose of retired external storage media in an environmentally sound way after purging data
- Provide VITA with the necessary documentation or certificates for external storage media that was disposed of
- Operate and support the media library and library management system.

Unisys understands CoV's compliance rules (e.g., COV SEC 514) for wiping and erasing data and configuration information that resides in the computer system, storage components, and devices complying with VITA Rules and before disposing of equipment. Unisys will support Customer-specific legacy backup systems for recovery of archived tapes or virtual tapes because various legal or legislative holds may surpass the availability of the physical backup infrastructure being used.

Unisys will provide reports of retired and disposed external Storage media in accordance with the SMM. Unisys will maintain an existing inventory control system to properly manage external storage in the media library and prepare it for shipment to the DR site.

Unisys will leverage the current offsite and media transportation vendor for storing external storage media. The current offsite vendor is expected to provide offsite vault storage in a physically and environmentally controlled and protected area with appropriate fire protection and multiple layers of physical security designed to prevent unauthorized access.

## 8.2 Backup and Recovery Services

Unisys understands that backup is one of the most important elements of a Recovery Plan. If a proper backup strategy is not in place to safeguard the critical data, data may be lost. Lost data can have an adverse effect on an organization in the form of a financial impact such as loss of business, legal actions, and low productivity. Therefore, it is imperative to have a robust backup solution and strategy in place.

Unisys will perform daily backup operations based on VITA's backup policies and industry best practices. Unisys will align the backup strategy to meet VITA's business and technical requirements. The backup strategy defines the schedule and type of backups performed, the processes for handling onsite backups and tape swapping (if applicable), and the processes for monitoring backups and resolving issues. Unisys will backup servers, databases, and storage devices up according to the predefined backup strategy.

Unisys' Backup and Restore Service will provide [REDACTED] management of VITA's backup environment. The service will monitor VITA's backup infrastructure, cataloging of backups, and restoring data from the backups and will keep it available in accordance with Unisys' standard SLAs. Unisys will perform system data backup and recovery with standard backup schedules and in accordance with VITA rules and the SMM.

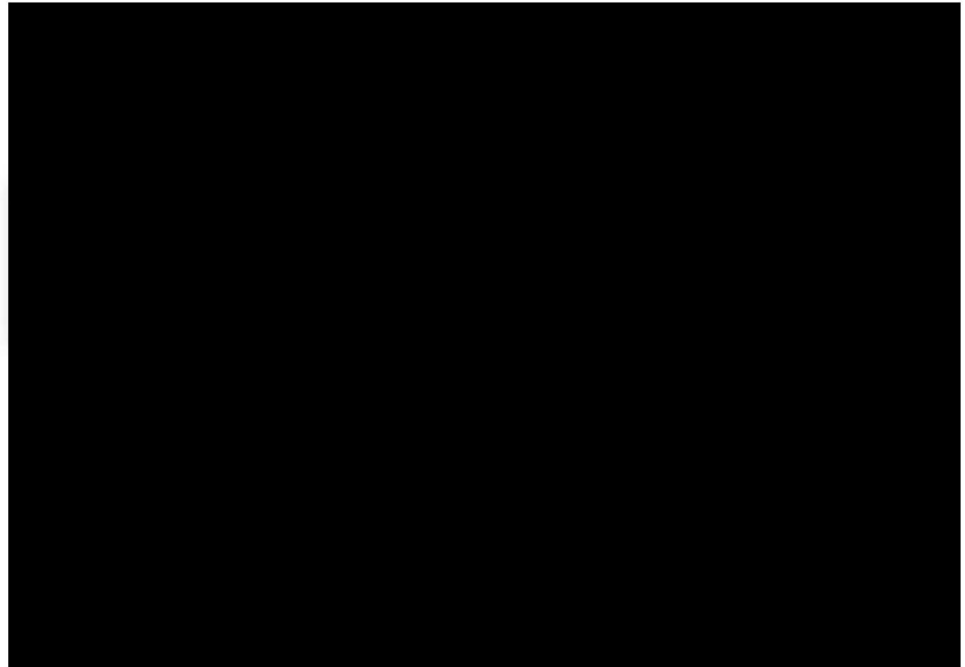
Unisys Backup and Recovery Service staff will provide migration services for existing backup devices residing at CESC and the secondary data center to bring them under Unisys Backup and Recovery Service management. Our Backup



and Recovery Service will manage current and future on-premise backup landscape and backup backed up to public cloud storage. Section 2.4, Implementation Plan documents how Unisys will manage the CMO and strategize the migration of workloads to FMO.

Unisys FMO Backup Services **Figure 8.2-1** will provide a comprehensive approach to data protection, which meets VITA's backup service requirements and SLA.

The services will also address Disaster Recovery Services across platforms and VITA's formally defined DR planning requirements (Business Continuity Plan, annual test plan, infrastructure, and facilities to which recovery can be made). Every day, Unisys will bring transparency and accurate real-time data reports to VITA, the MSI, and VITA Customers transparency and



**Figure 8.2-1. Backup Target Landscape (FMO).**

accurate real-time reports that document backup success and failure by filtered customer. Initiation and completion of restoration from backup will occur within the time defined in the service levels or within a shorter time in accordance with a user request. In addition to reporting, Unisys will develop a backup and recovery process and document the process in the SMM as well as maintain a list of servers to be included in the regular backup process.

Unisys' backup offering will bring the following benefits to VITA in our IaaS service offerings:

- Agility, flexibility, and scalability
- Standardization
- Unified management
- Durability and availability
- Encryption of data at rest.

Unisys will provide backup-specific reports and understands that the data used to generate the reports must be in a format that can be delivered to the MSI for warehousing and be broken out by Customer and service.

Unisys is relying on VITA to perform the following activities to support backup services

- If file locks occur due to VITA or Customer applications or databases, assist in troubleshooting
- Provide appropriate maintenance windows to support upgrades, patching and remediation activities

### **8.3 Provisioning and De-Provisioning of Storage**



Unisys' storage offering can provide HA of data in the DCs. Our storage offering provides a mechanism for VITA and its customers to expand or remove Storage Services as needed to meet requirements with automated workflow for Storage Service provisioning and deprovisioning that integrates with the MSI's Service Management Systems. This allows the capability to provision Storage that allows VITA and its customers to pay for storage consumed instead of storage allocated.

Data replication is enabled to serve the purpose of multisite replication such as DR. Our proposed approach comprises of setting up a redundant storage method to redistribute the data among different available data access patterns.

Different storage classes are defined and will be provided by different storage technologies that are integrated with VITA's Infrastructure Service.

Unisys will adhere to VITA and its customers' security policies for the destruction of data after deprovisioning request is authorized. Wipe and erase of the data and configuration information in storage, storage components, and devices will be performed in accordance with VITA rules and the SMM before removing or reallocating.

## 8.4 Security and Data Management

Unisys proposes security and data management that complies with VITA rules and includes data and data archiving. Our Storage, Backup, and Archive solution provides data management support, including creation or updates of SMM procedures for performing storage and data management and archiving that meet requirements and conform to defined policies. Our solution allows for the archiving of data based on various criteria (e.g., last accessed date, specifically on the current 30-day retention or 12-month retention. Our solution also provides access to data and backups that allows for cost-effective storage. The service brings out design and documents in the SMM and implements a data life cycle management plan based on VITA and its customers, specifically Library of Virginia requirements or regulations.

For more details on Backup and Recovery services, refer to Section 8.2, which describes the service and how Unisys leverages industry best practices for managing and organizing VITA and VITA customer data.

## 9.0 Network Services Associated with Server/Platform/Storage Services

Unisys will use [REDACTED] from assumption of service on December 2018 until Unisys has deployed ITSM tool ITOM for Asset Discovery and population in CMDB. Our proposed go-live of the new Asset Management System will be effective from the beginning of April 2019. The functionality of our ITSM tool solution will include discovery of enterprise assets that will be replicated in the MSI's ITSM tool instance at the B2B interface.

During the Implementation phase, Unisys will perform discovery, shadowing, and knowledge transfer activities to establish the foundation to assume service operations duties at Commencement of Services. Management of [REDACTED]

[REDACTED] is not in scope to Unisys. These activities align our practices with current functions and enable us to assume control and responsibility of services immediately. Upon Commencement of Services, Unisys Managed Network Services support will manage VITA's network devices at the primary DC as well as DR that support servers, platform, and storage. Unisys will provide network management support

throughout the life cycle of servers, server appliances, and platform-specific infrastructure, as shown in **Figure 9.0-1** from installation to decommissioning. Unisys' partner QTS has responsibility for CESC facilities and Unisys has responsibility of the Customer, CESC, QTS, secondary datacenter LAN environment(s).

In this transfer of responsibility of services to Unisys, Unisys will utilize VITA's existing hardware, software and tools to manage the environment. Once the environment is under Unisys management, Unisys will evaluate the environment, suggest improvements; as well as implement Unisys tools such as [REDACTED]. During this time, considerations will be made to phase out any VITA tools that should overlap with Unisys tools. These plans will be reviewed with VITA for approval.

The network layer for the new DC and DR is designed to provide greater agility and flexibility using a software-defined networking (SDN) architecture. Our CMP will be able to leverage its centralized controller that automates and orchestrates workflows using RESTful APIs.

SDN will provide multitenancy that uses the two delivery models that are operational in today's DCs: the underlay and overlay models.

Unisys will be responsible for network devices up to the core switch at the DCs, which includes the devices in **Figure 9.0-2**.

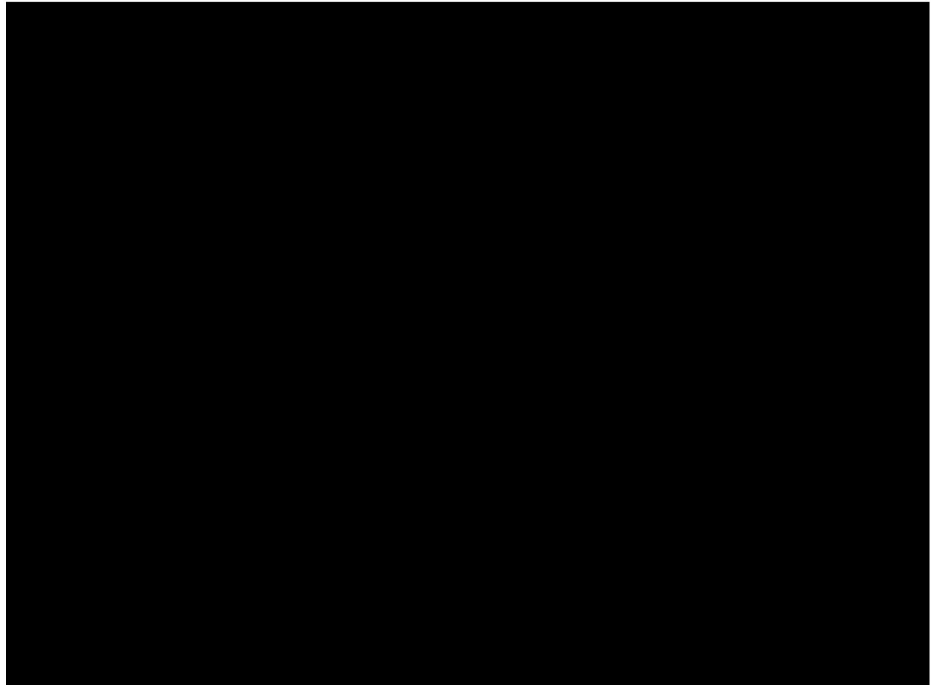


Figure 9.0-1. Using SDN to Support FMO Data Center Services.

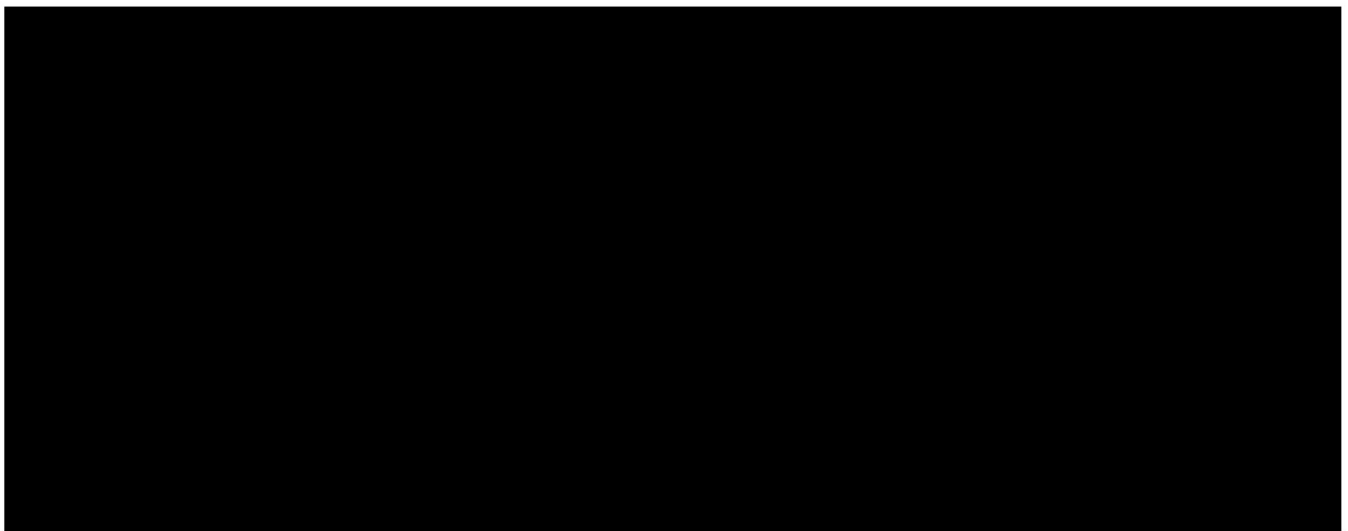


Figure 9.0-2. Data Center Network Conceptual Architecture.

- Local Area Network Services – The LAN will be deployed in spine leaf architecture, which has the advantage of easy scalability and centrally control by the SDN controller.
- Networked Appliance Services – Network appliances will include NTP Stratum 1 server as well as a DNS, DHCP, and IPAM server.
- Load Balancing Services
- Private Network Services – Our proposed network uses virtual pod (vPod) technology. BCF can create isolated “logical pod” fabrics, each with different orchestration (VMware, OpenStack, and containers), which are ideal for managed private clouds, engineering (Dev and Test) environments.
- Network Time Services – [REDACTED] to provide Stratum 1 Network time services
- IP Address Management Services – [REDACTED] [REDACTED] that can provide DNS, DHCP, and IPAM services are included.
- DC LAN Performance Monitoring and Management Services – [REDACTED] will be used to provide network monitoring and management along with ITSM tool ITSM toolset. For more information, refer to Section 2.3.

Unisys is relying on VITA to perform the following activities to support capacity management:

- Provide appropriate maintenance windows to support upgrades, patching and remediation activities

## 9.1 General Requirements

As described in Section 2.3, Unisys will assume service operations at Commencement of Services for console operations, monitoring, and management for servers, platform, storage, and related network infrastructure. Unisys provided tools will be integrated with the MSI dashboard and reporting systems that enable visibility and access to monitoring data and automated system-generated ticketing.

Unisys’ Managed Network Services technical team will act as a SPOC for network services and provide day-to-day operational support and administration for DC LANs. Network services also include installation of upgrades, configuration and fine-tuning, IOS upgrades, patching, and continuous configuration and updating of routing protocols and rules.

Our Network Operations team will update the operational documents in accordance with the SMM.

## 9.2 Planning and Design Services

During the development of new services, new technology evaluations, and service updates, the Unisys Architecture team follows a service design process that assesses the functional and nonfunctional requirements, including compliance, security, availability, service levels, redundancy, service continuity, and performance. Unisys also participates in and provides support for Architecture Work Groups (AWGs) and VITA Architectural Review (VAR) sessions to support design activities for new services and improvements for existing services. Unisys will use industry-standard steps and procedures to redesign the existing network to meet VITA’s requirements for an “as-a-service” model with the SDN-enabled network design described in Section 9.0.

**Planning:** A detailed analysis of requirements (e.g., needs of applications and interfaces with existing systems) will be evaluated. This provides the basis for making decisions when designing the solution. The Unisys project manager and technical team will coordinate with the MSI, VITA, and ITISP Governance to analyze the DCLAN



Service Equipment and Network's needs to build a detailed Implementation Plan to meet this engagement's needs.

**Assessment:** This phase includes a deep assessment of VITA's environment, taking existing knowledge from the incumbent into account and a detailed assessment of CMO to map it to FMO.

**Design:** This phase includes technical elements such as developing the system architecture; identifying standards (e.g., IP addressing, VLANs, routing, 802.11x); generating IP schemas; VLANs. The design will provide high-level and low-level diagrams that indicate the interconnection of related software and hardware components; overall network topology, including the physical and logical layout of the DC LANs; IP addressing; device/host naming schemas; security compliance; selected protocols for optimal communication on the DC LANs as necessary to satisfy VITA's and its customers' business; proposed network equipment, software, appliances, and services; network bandwidth and volume assumptions and projections; a performance plan; QoS design; and availability expectations based on the redundancy design and mechanism.

**Implementation:** Once the hardware is ordered and reaches the site, a Unisys CE is dispatched to work under the instruction of the Unisys Implementation Services Team on simple tasks that are required to enable the site devices and prepare them for remote takeover and configuration. As soon as a device is available for remote takeover, the Unisys Team will complete configuration and deployment remotely.

**Testing:** Once deployment is complete, UAT is performed to confirm that deployed solution works in accordance with VITA's requirements and satisfaction.

**Optimization:** Optimization of newly deployed infrastructure will be done for agility, cost reduction, and ease of operations as an ongoing activity.

**Management:** Unisys will manage network infrastructure as described in Section 2.3, provide proposal requested by VITA for new equipment or changes to the existing DC LAN Service environment, and develop and propose new or enhanced plans and designs continuously.

## 9.3 Operations and Maintenance

As described in Sections 2.3 and 9.0, Unisys assumes service operations at Commencement of Services for console operations, monitoring, and management for servers, platform, storage, and related network infrastructure.

## 9.4 Monitoring

Refer to Sections 2.3 and 9.9.

## 9.5 Network-based Appliance Services

Infrastructure security management is key to protecting VITA and its customers. Unisys will administer, monitor, manage and continually check for updates and overall system health. Unisys understands that the Managed Security Services provider will provide security monitoring for alerting and reporting to the MSI. Unisys will integrate the following Unisys managed device types with the SIEM tools to enable effective monitoring and management of the security ecosystem:

- Client VPN appliances

- Load balancer appliances

## 9.6 Third Party Network Services

Unisys assumes service operations at Commencement of Services for the existing third-party services and provides the available capabilities at CESC and the secondary data center. At the new primary DC at QTS and the secondary data center, Unisys will provide the required isolation of cabinets, locking of cabinets, fault-tolerant power feeds, adequate cooling and power to cabinets, and personnel logs as requested.

## 9.7 Network Time Services

Unisys understands that maintaining network time is important for applications, monitoring, and data consistency. Using [REDACTED] with a GPS antenna, Unisys will provide Stratum 1 NTP services for VITA with support for IPv4 and IPv6. Key platforms such as network devices, AD domain controllers, and UNIX systems are configured to rely on the NTP service. Systems using AD use the domain controllers for time and will be maintained one stratum lower. Access for NTP is available for VITA Suppliers in the environment.

## 9.8 IP Address Management Services

Unisys will use the existing [REDACTED] system at VITA that was recently refreshed to provide IPAM services. At Commencement of Services, Unisys will assume service operations for the existing [REDACTED] [REDACTED] to provide the requirements listed in the SOW that includes all changes, assignments of new static IP addresses, new site ranges for internal and external IP address ranges.

## 9.9 Data Center LAN Performance Monitoring and Management Services

As described in Section 2.3, Unisys will assume service operations at Commencement of Services for console operations, monitoring, and management for servers, platform, storage, and related network infrastructure. Unisys provided tools will be integrated with the MSI dashboard and reporting systems that enable visibility and access to monitoring data and automated system-generated ticketing.

[REDACTED] Network Performance Monitor will be deployed to provide monitoring compliance with Service Levels, service degradation, including detection, isolation, diagnosis, and correction of incidents 24x7. The [REDACTED] Network Performance Monitor has the following features:

- Hop-by-hop network critical path analysis regardless of device location—on-premise, hybrid networks, and the cloud
- Deep Packet Inspection and Analysis: Identify network and application latency issues
- New and improved user interface for better usability and navigation experience
- Native integration with ITSM tool
- Wireless Heat Map: Visualize wireless signal strength and location of connected clients.

## 9.10 Remote Access Services

### 9.10.1 General Requirements

The Unisys Remote Access Services with integration with AD and Identity Management will provide for secure, reliable and highly available remote access connectivity into DC core networks from other networks, VITA customer networks, the Internet, and other industry standard-based third-party vendor networks. As described in section 4.0, the Directory Services team will manage all access and will coordinate with Network engineers on the resolution of any network device issues.

### 9.10.2 Remote Access and VPN Security

For information on the MFA and [REDACTED] service used for secure access, refer to Section 4.4 and 4.8.

Unisys will provide VPN Service and support along with the following activities:

- Engineer, design, implement, and support VPN Services necessary to comply with VITA security standards
- Procure, implement, maintain, and monitor VPN Equipment (VPN Gateways, Servers and peripherals)
- Perform maintenance and upgrades on VPN Services and Infrastructure, including storage management, gateways and server systems administration
- Provide capacity management included License and hardware capacity
- Monitor VPN systems
- Respond to alarms and manage corrective action
- Work with End User service provider on Client VPN installation
- Provide operation support, including collaboration with MSI helpdesk for VPN related incident.

### 9.10.3 Remote User VPN

As outlined in VITA's DC network environment overview in Section 2.7, Unisys will use the same approach with [REDACTED] VPN client to provide fast, reliable, and secure access.

### 9.10.4 Remote User VPN (clientless)

The Unisys solution will use [REDACTED] for clientless SSL VPN. The [REDACTED] will be configured to allow clientless SSL VPN access [REDACTED]. A clientless SSL VPN [REDACTED] allows for limited, but valuable, secure access [REDACTED]. Users can achieve secure browser-based access [REDACTED]. No additional client is needed to gain access [REDACTED]. The access is provided using a [REDACTED].

Clientless SSL VPN provides secure and easy access to a broad range of web resources as well as web-enabled and legacy applications from computers that can reach HTTP sites.

## 9.11 Network Switching in Data Center

Refer to [\*Section 9.0.\*](#)

## 10.0 Disaster Recovery Services

When dealing with DR, it is important to focus on the end goal, which is the recovery of the critical application while maintaining the RPO and RTO levels when a disaster strikes. Unisys will use the following conceptual



architecture, working with VITA to shift the focus to include infrastructure, application, and business services as part of the overall DR Plan and related run books. DR services include planning activities, which include understanding elements of the COOP that affect the DR plan and related technical elements; identifying the DR scenario and RPO/RTO for each application requiring DR; using the right server hosting solution, including cloud, on-demand hosting, or dedicated servers to support the scenario, performance, and security controls for each system; using the right storage tier, replication, and restoration solutions based on the scenario and hosting solution; and developing the DR plan and run books to maintain a successful execution of tests and DR events.

Unisys will provide four tiers of service for DR using the RPOs and RTOs in Figure 10.0-1. The Data Protection and Recovery function is the data replication or backup solution that supports the RPO described. When combined with the server solution selected for DR Planning activities, the Infrastructure RTO will focus on the recovery of the infrastructure and application components before transferring the recovered systems to VITA and its customers' application support teams to perform their recovery activities within the estimated Application RTO. During an actual disaster (declared by CoV CIO), the usable data for the recovery may use older data (2 to 3 times the target RPO) because of corruption or incomplete transfers of the protected data before the disaster.

DR Tier	Data Protection and Recovery	Recovery (OS/Data )	RPO	RTO
1	Asynchronous Data Replication	Active Server or Replicated OS/ Replication	1 to 4 Hours	<4 Hours
2	Asynchronous Data Replication	Replicated OS/ Replication	<6-Hour Data Loss	5 - 24 hours
3	Disk-Based Nightly Backup	Client Restore/Data Restore	<24-Hour Data Loss	25 - 48 Hours
4	Disk-Based Nightly Backup	Client Restore/Data Restore	<24-Hour Data Loss	49 - 72 Hours

**Figure 10.0-1. Disaster Recovery Tiers and RTO/RPO.** Options support VITA business needs on premise and in the cloud.

Unisys also provides flexibility to change DR Tier (e.g., change between Tiers 1 to 2) using the same Data Protection capability based on business and operating needs. For example, a Customer has an application that requires a higher level of RTO and RPO for 4 months of the year. Unisys will work with the MSI and VITA to set up the structure and operating parameters to manage this move as part of the Demand Plan, Capacity Management, and operational standards. This structure enables the Customer to meet its key business cycles and needs and prevent the need to order higher cost services.

## 10.1 General Services

Unisys understands the MSI's role and responsibility in providing the management, planning, strategy, and testing coordination services associates with Service Continuity Planning. Unisys will provision the Infrastructure Services to align with the MSI's Service Continuity Planning.

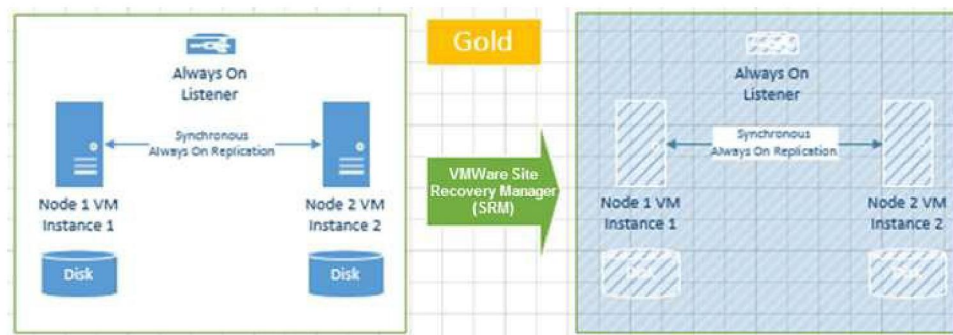
Unisys will explore cloud-based DRaaS or Recovery as a Service as long as required RPO and RTO requirements can be satisfied and GOV FISMA High satisfies VITA Rules. This will allow more flexibility for individual agencies to test or declare a disaster.

Unisys' network service includes the provision of DR network infrastructure and connectivity to a DC for backup and replication to support compute and storage requirements and meet RTO and RPO timelines. DR network infrastructure will be similar to that for DCs, but smaller in scale. Section 3.3 describes Inter-DC WAN connectivity.

VMware Site Recovery Manager (SRM) will be configured for Tier 2 FMO workloads to provide the automated DR recovery service for mission-critical services. VMware SRM will provide manual, semiautomated, and

automated DR by using vSAN or SAN array replicated storage. VMware SRM provides the capability to initiate a DR for set of protected workloads or the protected workload group. This brings the ease of using DR for only a set of protected workloads if necessary. SRM manual automated, semiautomated, and full-automated capabilities help VITA to leverage different RTOs and RPOs. Depending on the criticality of the workloads. Existing DR services will be factored for the VMware SRM Tier 2. The FMO vSphere environment Tier 2 and Tier 3 will have [REDACTED] HA and DS factored into the design to provide necessary HA. The solution will factor the N+1 availability design principle to maintain system availability during an unplanned outage of the underlying hardware.

Unisys database service includes the provision of DR infrastructure for databases to cover the required RTO and RPO requirements. As shown in **Figure 10.1-1**, VMware SRM orchestrates the recovery plan for SQL Server Disaster Recovery. Refer to Section 4, Implementation Plan for information on how Unisys will manage the CMO and strategize the migration of workloads to FMO.



**Figure 10.1-1. VMware Site Recovery Manager Database Recovery.**

Unisys storage and backup service includes the provision of DR to cover the required RTO and RPO requirements. The storage solution is catering to 100 percent replication of data for the tiers. Backup is considered for the tiers and replicated to the secondary data center. In this way, Unisys backup solution provides online and offsite backup.

Unisys' backup solution is based on a 100 percent tapeless solution. Data for long-time archiving solutions on cloud-based DR models must be chosen carefully, considering the data is cold, with no hot and warm data. This is key for cost reductions on the link because data moving from the public cloud has a heavy cost from the cloud provider and the respective network link usage. Refer to Section 2.4, Implementation Plan document for information on how Unisys will manage CMO and strategize the migration of workloads to FMO.

## 10.2 Disaster Recovery Planning and Testing Support

Unisys will collaborate with VITA in providing the management, planning, strategy, testing, and coordination of DR and Service Continuity Planning. Unisys will jointly develop and manage a strategy to enable RTOs and RPOs to be met. During the Implementation phase, Unisys will develop a comprehensive DR procedure jointly with VITA and the MSI to support VITA and VITA customer-specific work instructions outlining the procedures for planning, testing, declaration, implementation, failback, postmortem and continuous improvement processes. This also will include performing DR Site capacity planning, tests of fallback activities, and Change Management on changes that are required for maintenance and that occur during the execution of the DR Plan as well as maintaining the DR run books at a secure remote location that is accessible outside the primary DC.



Unisys will coordinate with the MSI, VITA, and VITA Customers to receive updates to business requirements and threats to augment or modify the DR plans. Updates will be in accordance with the procedures outlined in the SMM.

As part of transparency and reporting, Unisys will provide the MSI with DR testing status for IT Applications, including when a DR plan was last exercised and the status of that test, and support a comprehensive DR testing schedule. Unisys will provide the DR strategy with input as required by the MSI, VITA, and its customers and recommend solutions to close gaps in the Lessons Learned Report.

The DR Plan will be updated in infrastructure or applications change work with the MSI, VITA, and VITA customers. With expertise in multiple DR engagements, Unisys will provide the necessary qualified resources to support DR planning, improvement, and testing, preventing single points of failure of DR personnel with defining Supplier roles, responsibilities, and a reporting hierarchy for the different DR teams and members, and maintaining reporting structure diagrams. Unisys will also conduct scheduled training of DR staff as applicable.

Unisys is relying on VITA to perform the following activities to support disaster recovery services:

- Provide and update a list of critical applications and associated RTO/RPO
- Provide notification of changes in applications that may impact disaster recovery procedures or capabilities

## **11.0 Security Functions**

### **11.1 General Integration**

When dealing with Security Functions, it is important to consider a documented information security policy and implement adequate procedures to protect the confidentiality, integrity, and availability of VITA's assets and confidential data. This is vital because VITA is required to develop, implement, and maintain administrative, technical and physical safeguards for the elements, of its enterprise compute, network, cybersecurity, and storage ecosystems. These procedures and safeguards must reflect industry best practices. VITA Suppliers and the agencies they support must update their procedures and safeguards at least once annually and more often, if necessary, to remain compliant with industry standards, industry best practices, and applicable laws and regulations.

Features of the Unisys offering for Security Functions include general integration, end point security, data security, and application security. Unisys will work closely with MSS to implement security measures on Unisys managed devices.

### **11.2 Endpoint Security**

Unisys will install VITA Managed Security provided end point security solution as directed by STS.



### 11.2.1 Full Disk Encryption

Unisys will implement full disk encryption as required by VITA Rules and in accordance with the SMM. Software encryption is enabled on the storage and backup devices that maintains data encryption at rest and data encryption in motion. Storage and backup replication has data encryption that is motion enabled. When VITA replicates data from an encrypted system, the data is decrypted before it is replicated. Data is encrypted on the destination system if encryption is enabled on that system. Security and network devices support encryption on the WAN link. Storage and backup devices provide the ability to perform a forensic analysis of the encrypted data. The device must be able to be decrypted with the forensic software to support the forensic analysis. The Unisys proposed solution is based on end-to-end FIPS-140-2 compliant and industry standard [REDACTED] validated [REDACTED] [REDACTED] for encrypting and decrypting stored data.

## 11.3 Data Security

### 11.3.1 Enhanced Database Security (EDS) Service

Unisys will support the current EDS service. As previously stated in Section 7.3, Unisys will provide a database cloning platform that also provides a fast and consistent data masking capability that provides a consistent but anonymous version of personally identifiable information in the production database. The Unisys integrated platform is from our technology partner Delphix and part of the VITA solution.

## 11.4 Application Security

Unisys will support VITA's current secure file transfer systems and applications. We will support customer data files between an application as well as internal and external locations.

## 12.0 Enhanced Services

Unisys takes the approach of unifying the inventory information of application profiles, version management, data, underlying security and infrastructure with the business, regulatory inputs to arrive at applications recommendation for end state architecture fitment and migration.

Unisys will use a four-phase approach to take VITA through the journey of transition.

1. **Discover** – During this phase Unisys take approach of site visits to verify the physical assets , documented asset and inventory. Unisys will then apply tools like [REDACTED] to discover the infrastructure and application inventory details. Unisys will help to align the workloads with right tools with our time tested practices (Unisys IP application and infrastructure assessment toolkit) to maintain maximum efficiency and delivery speed.
2. **Analyze** – During this phase, security personnel gain insight to data residing in each system, the mission that each system supports, and its criticality to determine alignment with VITA Rules and NIST SP 800-53 security controls. Unisys will identify competencies and skills that map to strategies. Unisys will rely on multiple perspectives from several tools like [REDACTED] [REDACTED] to analyze the data from multiple directions.

3. **Strategize and Plan** – The success factors are identified along with alternate FMO (solution options), identification of high priority systems with customer key stakeholders and decision-making executives and management. Recommendations are provided to resolve risks, overcome constraints, retire systems, address security risks, and gain faster benefit realization. An implementation roadmap is developed from the higher priority initiatives identified, a funding sequencing plan is proposed, and a final report is compiled and presented that includes specific recommended action plans for specified time frames along with refactoring options.
4. **Transition and Operate** – Unisys will deploy the Unisys CMP, which is hybrid public and private cloud platform integrated with the Government ITSM processes and a CMDB to assure cloud governance framework that will address the cloud lifecycle's six domains: Application Architecture, Operations, Integration and Interoperability, Portfolio Management, Cloud Service Provider Management, and Finance Management.

Our Digital Transition framework provides the approach to minimize the risks while allowing for faster transition and realization of benefits in a systematic way by allowing Customers to make data-based decisions to maximize their benefits while transitioning to an operational expenditure-based model.

## 12.1 Cloud-Based Services

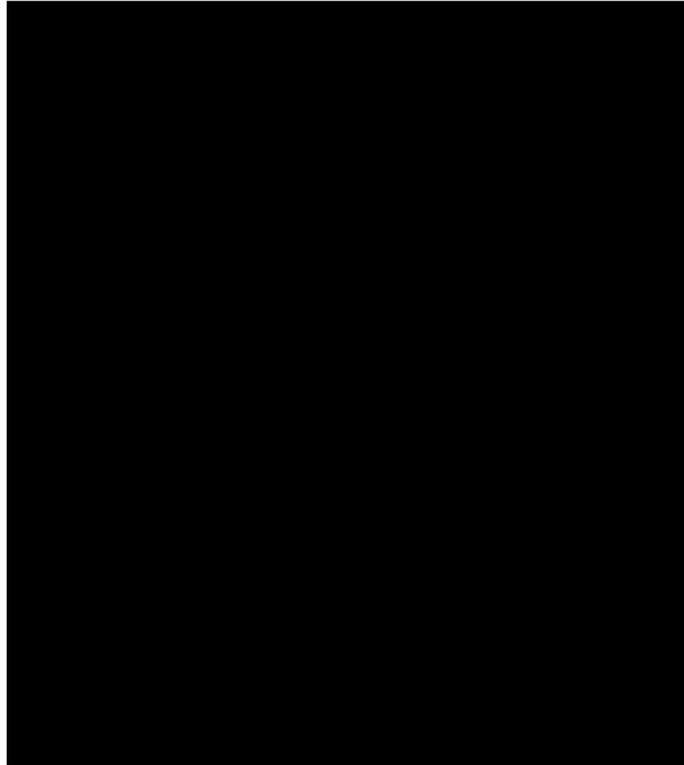
### 12.1.1 Public Cloud Services

Unisys Public Cloud Services will enable Agencies to transition from on-premise hosted applications to cloud hosted applications. Unisys and our partner ecosystem will assist Agencies with application migrations to the public cloud. Unisys will ensure all workloads in the cloud are compliant with SEC 525 (COV-Sensitive) security requirements through the Unisys managed services governed by VITA policies. Though this is a managed service, the Agency will have deployment options to support their application requirements. This solution consists of the use of the Oracle Government Cloud, Amazon Web Services ("AWS"), Microsoft Azure ("Azure") and the processes to enable management, delivery, operations and support of the environment.

#### Enterprise

VITA Agencies are looking to use cloud services to support their modernization efforts and to meet Executive Order 19. The solution consists of Unisys managed Platform as a Service (PaaS) with associated services provided by other VITA STS'. The component diagram is shown in the figure below. The figure shows a production depiction of the solution.

#### Unisys Public Cloud Service Solution



The core of the solution are the Cloud Service Providers (“CSP”) including AWS, Azure and Oracle Cloud Infrastructure (OCI) for Government Cloud , an integrated set of services providing cloud native a portal for transparency of the deployed services. The solution is being offered as a managed service provided by Unisys and its subcontractor.

The solution described within this document is being offered as a fully managed service. During the request process, a MSI provided work order will be completed by the Agency to communicate their requirements. The solution will also provide VITA with secure integration with services offered by the other STS’. In this design, all components of the solution will utilize the [REDACTED] for connectivity and Managed Security Services by the Commonwealth’s Managed Security Services provider.

### **Environment**

The solution will be hosted in one of the three CSP offerings . Unisys and CSP subject matter experts are available to assist Agencies with their application cloud strategy and modernization questions if needed. It is a critical goal of VITA to ensure any workload moving to the public cloud is optimized to use cloud services efficiently.

The solution components are hosted within a FedRAMP moderate authorized cloud ( FedRAMP website located at: <https://marketplace.fedramp.gov/#/products?sort=productName> ) subject to the physical and logical security controls necessary to maintain compliance with that authorization. While FedRAMP is not a stated Commonwealth requirement it does at minimum, meet all of the SEC525 security requirements to maintain a COV-Sensitive posture. In addition, the Commonwealth’s Voice and Data Network Services provider (VDN) will ensure all network access to these systems from the Internet is encrypted [REDACTED] [REDACTED] with the solution encrypting all data at rest via full disk encryption.



The Unisys Cloud service will be integrated with Okta and [REDACTED]. As part of the integration with Okta and Active Directory, [REDACTED] capabilities will be extended to the cloud. The addition, modification or deletion of user privileges will follow standard COV change control policies.

The Unisys solution itself will allow Agencies to tailor the services deployed via completion of the service request process through Keystone Edge. The following high level list depicts the services that will be available to the Agencies.

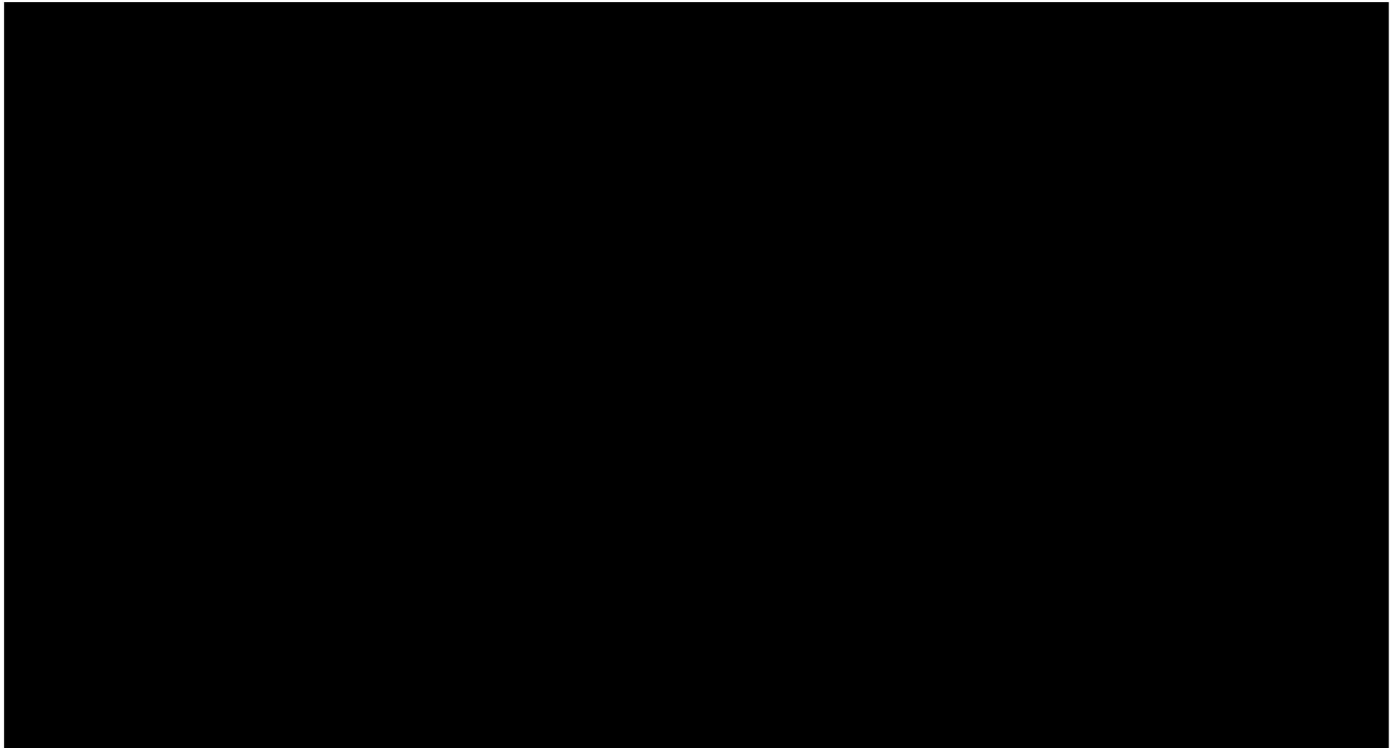
1. Number and configuration of virtual machines on IaaS
2. Platform as a Service
3. Backup
4. Disaster Recovery
5. High Availability
6. Cloud based licensing for database and applications
7. Bring your own licenses (BYOL) to the cloud
8. Off boarding options

This solution is available on AWS, Azure and OCI however to enable a hybrid environment the solution will take advantage of the existing service descriptions and resource units managed by Unisys. This section will detail the above offered services.

### **Disaster Recovery (DR), Backup & High Availability**

Disaster Recovery will be implemented in separate region or availability zone of the CSP. The solution is designed to allow Agencies to customize their requirements.

The solution and management of the solution is flexible to provide the right services based on Agency requirements. Unisys will collect the Agency requirements which will be reviewed by Unisys and the MSI. Unisys and MSI will provide any optimization recommendations for the Agency to consider based on the totality of their requirements. Below is a high level example of a multiple region solution using Oracle Cloud infrastructure. The same design concepts will be used for AWS and Azure.



### **Agency Off boarding**

It is always important for the COV to understand how to remove their data from a cloud service. This can include optional Unisys Migration Services available through the service catalog. This section will detail the offboarding process.

### **Termination of Oracle Cloud Services**

**For a period of 60 days upon termination** of Unisys Cloud Services, Unisys will make available, via secure protocols and in a structured, machine-readable format which will be determined prior to service provisioning, COV content residing in the production Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval. After 60 days there is no obligation by Unisys or CSP to retain COV Content after this retrieval period. Assistance is available from Unisys to obtain access to or copies of the data. A VCCC service request will need to be opened with Unisys working with the CSP support team to provide the required support. Following the expiry of the retrieval period, the CSP will delete the content from the Cloud Services environments (unless otherwise required by applicable law).

### **Destruction and wiping of data**

CSP instances are securely wiped after virtual assets are released by the COV. This secure wipe restores the underlying IaaS to a pristine state. The CSP will follow a media destruction process that adheres to VITA's Removal of Commonwealth From Electronic Media Standard ITRM Standard SEC 514-05

documentation. Decommissioned drives supporting IaaS and PaaS are degaussed and then physically destroyed using mechanical shredders.

12.1.2 Cloud Solution Components

To meet VITA’s cloud security and compliance requirements, Unisys partnered with stackArmor to provide cloud-based services. stackArmor developed a proven and systematic cloud transition approach called the Agile Cloud Transition (ACT). stackArmor’s principals successfully supported high-profile cloud migrations for the White House and the Recovery Accountability & Transparency Board (RATB) for Recovery.gov in 2009, Department of Defense (DoD), U.S. Department of the Treasury and many other state, local, and federal agencies. All architecture and design will be performed in compliance with VITA Sec 501 and 525 requirements and reviewed by the MSI for approval prior to moving forward.

Cloud Migration – Security by Design

stackArmor’s ACT framework in **Figure 12.1-1** will maintain the security and integrity of VITA’s data by architecting in compliance with VITA Rules as well as NIST SP 800-53. NIST SP 800-53 is a collection of controls that form the basis of the Federal Risk and Authorization Management Program (FedRAMP) and DoD Cloud Computing (CC)

Security Requirements Guide (SRG). Unisys and stackArmor will maintain the successful cloud modernization and migration to deliver cost efficiency, agility, and better operational security in compliance with VITA’s requirements. There are three key facets to Security by Design: These include creating a strong compliant architecture that meets

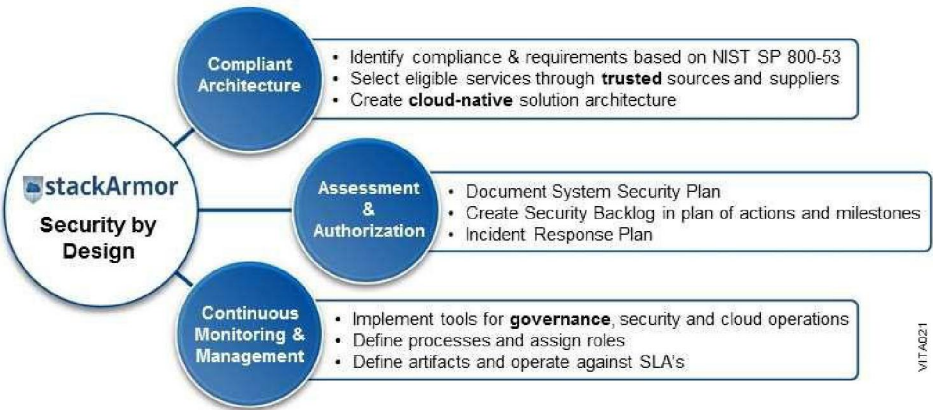


Figure 12.1-1. Act Framework for Security by Design.

compliance and regulatory standards; creation of a formal assessment and authorization framework with well-documented policies, procedures, and practices to provide security using a shared responsibility model; and a robust continuous monitoring program.

Cloud Security and Compliance based on Government Best Practices

Unisys and stackArmor have a strong understanding of the holistic security and compliance framework described in **Figure 12.1-2** with relevant adaptations for commercial cloud platforms such as AWS, OCI and Azure that will enable adequate satisfaction of VITA’s Sec 501 and 525 security and compliance requirements. Unisys and our partners maintain the following compliance with Federal standards and will translate those to SEC 501 and 525.

Publication	Brief Description	Relevance to VITA Cloud Computing Migration
-------------	-------------------	---



FIPS 199	Standards for Security Categorization of Information Systems	Helps VITA to make a fact-based risk assessment based on confidentiality, integrity, and availability dimensions categorized as High, Moderate, or Low.
NIST SP 800-53	Security Controls and Assessment Procedures for Information Systems and Organizations	Helps VITA to implement a standardized set of controls for protecting and securing cloud based applications and data.
NIST SP 800-160	Secure Systems Engineering Practices	Implementation of Controls must follow industry best practices as specified by experts.
NIST SP 800-37	Information Security Continuous Monitoring (ISCM)	Implementation of continuous compliance and monitoring of controls and compliance architecture

**Figure 12.1-2. Strong Foundational Security and Compliance Framework.** *This framework is adapted for commercial cloud systems based on international and national standards.*

Since 2009, stackArmor has successfully architected and executed large systems migrations to the AWS and Azure platforms and will bring the same level of expertise to VITA's Private and Public Cloud Computing Migration and Modernization Program through the shared responsibility model.

The infographic below shows the 6-step process to achieving a secure and compliant cloud platform based on national and international best practices and standards used by US Federal, DOD and State & Local Agencies.



**Figure 12.1-3. Risk Management Framework.** *For going through the Assessment and Authorization processes for commercial cloud systems with a shared responsibility model and controls inheritance from the CSP.*

### Solution Architecture – Compliant by Design

Given VITA's role in providing a broad range of enterprise IT services to the Commonwealth of Virginia (COV), as a shared services provider organization, the cloud computing platform for the COV must be vendor-agnostic and provide best of breed security protections. Unisys [REDACTED] is a unique cloud-based security service to help with creating micro-segmentation and hinder the ability to detect and penetrate cloud environments.

Each commercial cloud platform is monitored and secured using the Unisys [REDACTED] service. Additionally, using ITIL and industry best practices for Service Management, ITSM tool is fully integrated into the service fabric. Key features of our proposed solution architecture are provided below.

**Full-stack Security Architecture:** It is important that all layers of the system are considered when designing the corresponding architectural blueprints. In addition to the engineering and cloud architecture constructs, it is

essential to have a demonstrate security posture through the appropriate compliance documentation including policies, plans, and reports.

***Dedicated Enclaves with full-segregation and control for VITA:*** As part of the design is to provide clear separation of the various workloads and environments to allow for security, scalability and future expansion. The figure below provides a high-level overview of the architecture Unisys would propose for all CSPs.



**Figure 12.1-6. [REDACTED] design with a management, production, test & dev. supporting continuous monitoring services are integrated as well.**

**Design highly secure and hardened environment:** Unisys along with stackArmor have experience in designing multi-layered security architecture as described in the table below.

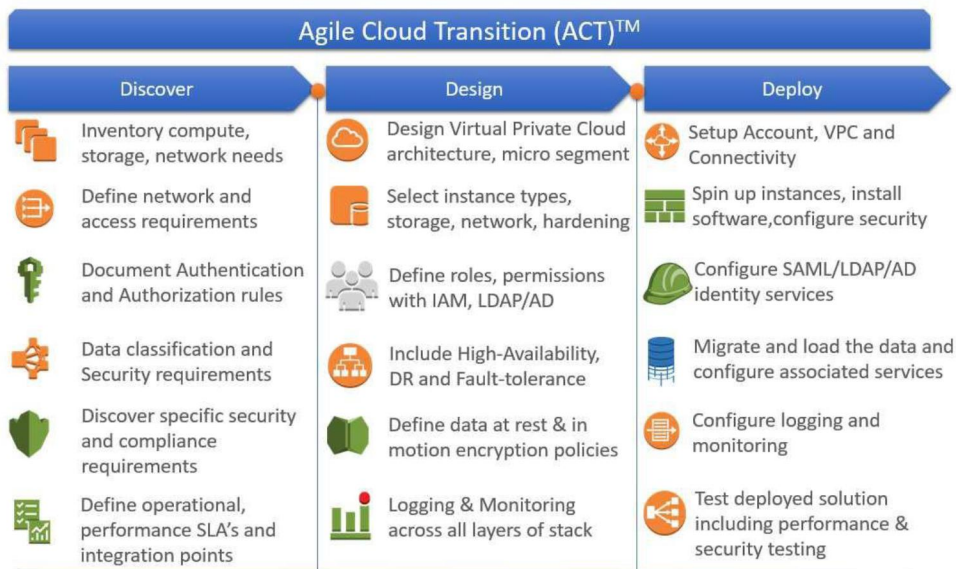
System Vulnerability	Preventative Security Measure
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]

**Continuous Integration/Continuous Deployment:** Design and incorporate modern automated CI/CD (DevOps) services with industry standard components such as Jenkins and Gitlab.

**Logging & Monitoring across all layers of the stack:** The design workstream includes leveraging various tools for the various aspects of the application, data and system platform that must be monitored.

### Transition Approach

The Unisys Transition Team will be staffed with senior and certified CSP Solutions Architects. Once the migration blueprint has been established, the actual migration activities can begin by iteratively executing sprints of discover, design and deploy cycles. The infographic below provides an overview of the sprints and activities.



**Figure 12.1-8. Overview of Sprints and Activities.** Agile Cloud Transition methodology for migrating VITA's Applications to a FedRAMP accredited Commercial Cloud Platform.

The phases are executed by experienced and certified qualified team members with multiple production deployments and well-defined roles & responsibilities. Each of the workstreams and their associated activities is described in greater detail below.

### Discover Phase

The Discover workstream is focused on detailed requirements analysis and ensuring the mapping of all of the application, data and infrastructure components and services to the target cloud service is performed.



**Cloud Compute, Storage and Network components:** The Discover phase requires creating an inventory of all compute, storage, network and associated infrastructure services. The inventory allows for an accurate estimation of cost and provides visibility for all stakeholders early in the process.

**Network and Access:** This includes understanding the user base of the applications and where they will be connecting from. The **Figure 12.1-9** below provide a logical view of the networking and aces configurations for both the AWS and Azure platforms.

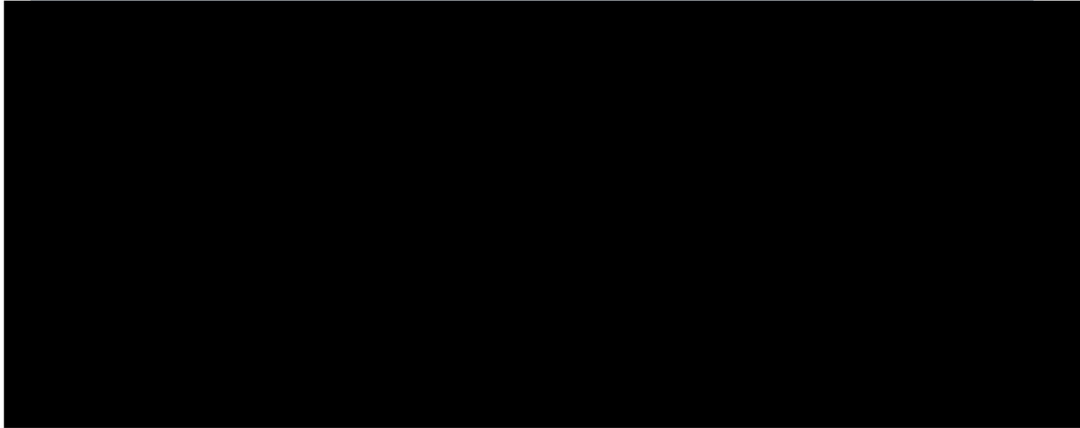


Figure 12.1-9. [REDACTED] connectivity to help extend data center into the cloud such as Azure from multiple VITA locations.

**Identity Management:** Delivering the right authentication and authorization service is necessary so that only authorized users have access to the infrastructure, application and data resources. Unisys will integrate with VITA Active Directory and [REDACTED] enterprise services.

**Data Classification and Protection:** The data resident in the various systems must be categorized in greater detail using Sec 501 and 525 procedures. The data is categorized and classified based on Confidentiality, Integrity and Availability attributes and rated into COV Sensitive or COV Non-Sensitive.

**Continuous Integration/Continuous Deployment:** This activity includes analyzing and reviewing the existing code repository and build as well as code deployment methods.

**Concept of Operation:** The ability to seamlessly operate and manage the cloud platform along with the applications requires a comprehensive concept of operations that is based on commercial best practices adapted for VITA requirements. It is important that the Unisys understand and interact with the key stakeholders within the VITA's Program Office associated with delivering business services as well as the key operational services including but not limited to ticketing and support, management reports, status dashboards and continuous improvement sprints.

During the discovery process Unisys rapidly interviews and reviews documents and tools available to help ensure that the various elements of operations and continuous improvement can be executed during the maintenance phase of the project.

An outcome and deliverable from the Discover phase are a **Systems Requirements Specification (SRS)** that captures the key findings and requirements of the program.

## Design

The Design phase is executed by a Senior CSP Solutions Architect in partnership with the Information Assurance (SME) to confirm that the CSP hosting environment is compliant and meets all of the business, technical and security requirements.

A key deliverable from the Design workstream is a System Design Specification (SDS) Document that captures the details of the **To Be built** solution to confirm compliance and user feedback and acceptance.

## Deploy

The Deploy workstream is the final rapid iterative, and intensive delivery focused activity that includes bi-weekly sprints. Each sprint includes incremental progress that helps deliver functionality to the customer based on the approved design. The overall approach and activity towards executing the actual stand-up and migration of the various components that begins with foundational services.

All along during this workstream, there are regular stand-up meetings to communicate progress and resolve issues rapidly. At the end of this phase, a fully working environment and application is stood that has been thoroughly tested and validated with the ability to obtain a formal ATO (Authority To Operate). The actual deployment is executing with the purpose of migrating and delivering rapid incremental value to avoid a disruptive big bang migration. The actual final sequencing of the migration is developed based on joint discussions with various stakeholders.

Our FMO solution comprises of a hybrid cloud underpinned by a single cloud management platform (CMP), using cloud-brokering services with private and public cloud. The Unisys solution will improve productivity through increased service delivery quality and reliability. The Cloud Management Platform (CMP) will provide the ability to manage the on premises private cloud hosted at QTS DC and the secondary data center along with the public cloud service provides like AWS and Azure. Unisys CMP will bring following Cloud management capabilities to the VITA infrastructure as part of its CMP.

- Orchestration and Rapid Deployment & Provision
- Self-Provisioning and DSC
- Third party Cloud Provider support
- Workload Analysis, Recommendations & Mapping
- Multi Source Integration (i.e. Client ITSM/SN)
- Analytics and Reporting

Unisys can manage public cloud vendors to the licensing discounts that Unisys enjoys through our strategic partnerships. The CMP is also flexible enough to use favorable software licensing terms that VITA may have negotiated with software and public cloud providers.

Our CMP is based on an industry leading platform, which maintains a universal cloud partnership with strategic public cloud vendors that brings VITA ready built access to a wide portfolio of public, private, and hybrid cloud services such as AWS, Azure, OCI and Google Cloud Platform on Rackspace, IBM SoftLayer clouds, Apache CloudStack, OpenStack, and VMware vSphere.

Nevertheless, in this diverse landscape, common operations are maintained to support uniformity and enterprise control. Unisys CMP uses standard build blueprints of cloud resources that VITA would easily build and deploy.

CMP provides a dashboard to configure, orchestrate, and establish visibility of deployed resources. It provides an automated provisioning API to integrate with public cloud and private cloud frameworks such as Windows Azure Pack, VMware, and OpenStack implementations. This support of diverse frameworks is important because it gives VITA a flexibility to onboard existing infrastructures without seeking new providers.

Therefore, the CMP not only provides automation and orchestration of new service provisioning, but it also offers a comprehensive Cloud Brokerage layer and a single portal for VITA business to request compute and cloud services, which can be extended for VITA IT Services.

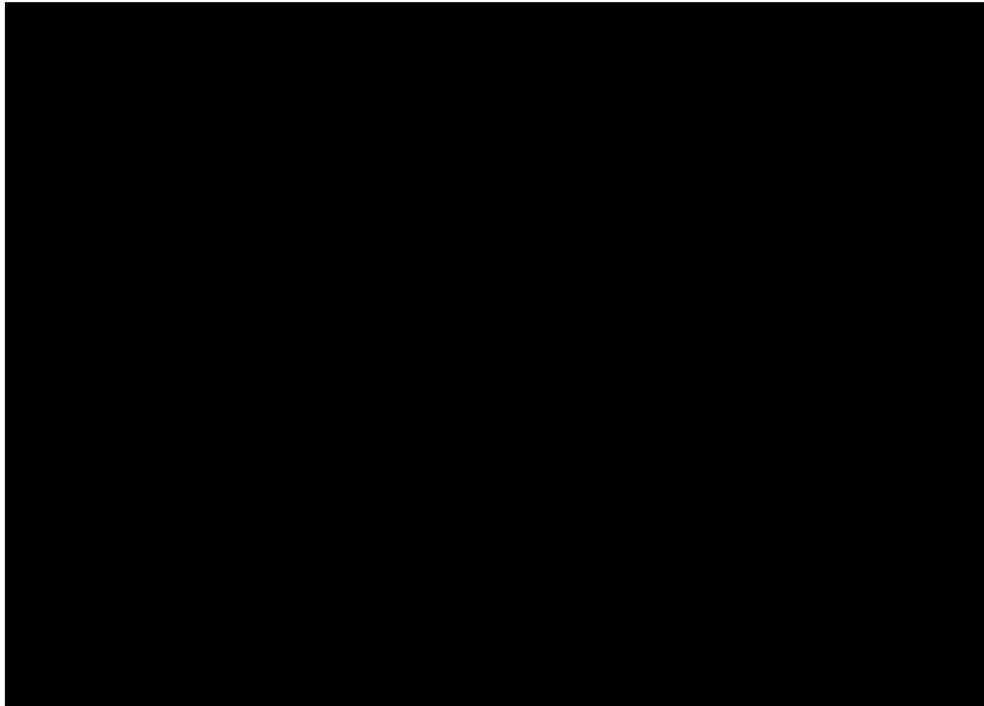
### 12.1.3 Cloud Optimization (Optimization as a Service)

#### Overview

The [REDACTED] platform enables the self-management of heterogeneous environments to ensure the performance of any application in any data center or cloud environment. The [REDACTED] dynamically analyzes application demand and allocates the full supply chain of all shared resources to all applications in real time, to maintain environments continuously in a healthy state.

The [REDACTED] instance is comprised of a patented [REDACTED] which uses real-time analytics gathered from instrumentation in the VMware [REDACTED] Server environment as well as the virtual and physical infrastructure, including the virtualized applications.

#### [REDACTED] logical architecture





Each of the [REDACTED] components operate within the [REDACTED], which is deployed on virtual or cloud infrastructure using an OVF deployment. Other formats are available to deploy within Microsoft Hyper-V, Red Hat Enterprise Virtualization, OpenStack and XenServer platforms.

The [REDACTED] can also be deployed in your Cloud accounts, and is available as an image [REDACTED].

### **[REDACTED] Presentation and Reporting**

The UI for [REDACTED] includes the HTML5 standard user interface. Reports extract data from the server in real time, and historical from the DB. All requests from the “new” UI leverage the API services layer so all actions and views in the new UI can be done through the API.

### **[REDACTED] API**

[REDACTED] presents two API options including the traditional API and the REST API, which represents the Services layer to access data, the Market, and even configuration details of the [REDACTED]. API extensions are being developed to provide complete feature parity via the RESTful API, and in some cases, providing API capabilities that will not be featured in the UI. [REDACTED] issues XML (traditional) and JSON requests (and responses), as well as full support for our Role-Based Access Control (RBAC) via the API.

### **[REDACTED] Analytics: Patented Economic Engine**

The core of [REDACTED] is referred to as [REDACTED]. The patented [REDACTED] applies economic principals of supply and demand to generate actions from virtual currency that assure performance while utilizing the infrastructure as efficiently as possible. The engine uses internal pricing of virtual commodities within the infrastructure to converge to the desired state the supply of resources against the demand of applications. Instrumentation is gathered via the [REDACTED] real-time probe process and fed into the [REDACTED] environment to provide actionable decisions based upon real-time analytics.

### **[REDACTED] Abstraction: Repository**

Using a common abstraction model, [REDACTED] is able to take the instrumentation from the virtual, cloud, and application infrastructure to represent the entities in [REDACTED] and construct the supply chain of buyers and sellers of commodities, or the supply chain of consumer of resources (such as virtual machines) with their providers (such as host and storage).

### **[REDACTED] Mediation**

Mediation takes in all the metrics, configuration and data required to understand supply and demand, and then in turn provides control capabilities into every layer of the infrastructure where the true value of [REDACTED] is realized. This sub-system interacts with the management components of the virtual, cloud, or application infrastructure, as well as with physical compute and storage. Mediation allows move, resize, provision, de-provision, deploy and scale actions to be performed.

### **[REDACTED] Database**

Data is maintained within the [REDACTED] instance to provide historical performance information both to the TAP environment and to the UI for consumers to pull reports and historical utilization information.

### **Architecting [REDACTED] in a Hybrid Model Deployment**

#### **[REDACTED] Architectural Elements**

The [REDACTED] is the heart of the [REDACTED] eco-system. It can be deployed as with standalone, multi-site or multi-region aggregated configurations. The [REDACTED] operates within the infrastructure as a virtual appliance on any supported hypervisor platform or as a SaaS implementation within the public cloud.

[REDACTED] is comprised of a set of core services, which include the patented Economic Scheduling Engine. Analytics are gathered in real time by probing management APIs of the target infrastructure, which provides actionable decisions for application, hypervisor, storage platform, network platform, and public cloud environments. The mediation layer provides a common abstraction to map elements into the [REDACTED] platform and to provide control capabilities in the target infrastructure.

#### **On-Premises Virtualization/Private Cloud Architectural Elements**

##### **Virtualization or Private Cloud Management Server**

This element is the management and control plane of your on-premises virtualization, private cloud platform and your Public Cloud deployment. It usually comprises of the Platform Services Controller(s), API front end and a Database.

For example, [REDACTED]

Most virtualization and private cloud solutions will use a hypervisor running on bare-metal servers, and use the management server to create clusters of resources. Each cluster will provide Recoverability, Availability, Manageability, Performance and Security functions for the Virtual Machines running in those clusters.

#### **Public Cloud Architectural Elements**

##### **Management Interface**

Public Clouds include a front-end management interface. This interface will include secure API endpoints for the various cloud services. Administrators and users can interact with the endpoints using UI Console, CLI, or scripts / automation tools that leverage the respected cloud APIs.

##### **Global Infrastructure**

Public Cloud Global Infrastructure is consisted of multiple geographical locations called Regions. These regions provide compute, storage and network services to the public cloud tenants. Azure uses the concept of Regions only while AWS divides their Regions into sub-components called Availability Zones (AZ), which represents different datacenters in the same geographical area.

##### **Physical Hardware Architectural Elements**

Server: Bare-metal compute infrastructure comprised of motherboard, CPU, RAM and storage/network interface cards.

Network: Layer-2 and Layer-3 network devices that have the ability to switch frames and route packets.

Storage: Systems comprised of disk arrays that provide remote, centralized storage or software-defined storage to be consumed by [REDACTED].

Security: Appliances and software that provide defense in depth with security functions such as layer-3 filtering, intrusion prevention, intrusion detection, end-point protection, malware detection, email scanning and application filtering.

Authentication & Authorization: The [REDACTED] allows for role-based access controls. Users are only able to access information to which they have been authorized. Authorization may be based on several things including responsibilities and authority within the organization. Roles are easily created, altered or ended as the requirements of the business change, without needing to individually update the access privileges for every employee. The [REDACTED] also integrates with LDAP groups.

Log Collection: Administrators can view logs of activity information for all users, including user creation, logins, and changes to the user's record within the logs provided on the [REDACTED] server

High Availability: [REDACTED] can be configured in an active/active HA configuration by using two Turbonomic servers connected to the same targets with the same policies. Only one Turbonomic server should be taking actual action

Backup & Recovery: Solutions that provide image-level backups, filesystem backups, database and application consistent backups.

#### 12.1.4 Unisys [REDACTED]®

##### [REDACTED]® OVERVIEW

VITA is seeking a public cloud security architecture to protect Commonwealth data, people and assets using a combination of Software as a Service (SaaS), cloud-native services and security software hosted in the cloud conforming to Sec-525. Unisys is proposing a solution that will efficiently integrate with the existing Commonwealth of Virginia and ATOS Managed Security Services (MSS) solutions to complete an end-to-end security model.

In a hybrid environment, Agencies and their developers will not have to navigate one set of security for on-premise workloads and another set in the public cloud. Navigating the different rules and policies impacts performance and could lead to risk and customer frustration.

Using [REDACTED]® will assist VITA “Future Proof” your preparation for NIST 800-207, which is now in draft. NIST 800-207 is the Zero Trust NIST standard which states:

*“...Authentication and authorization (both user and device) are discrete functions performed before a session to an enterprise resource is established...”*



*“...Zero trust focus on protecting resources, not network segments, as the network location is no longer seen as the prime component to the security posture of the resource...”*

Unisys [REDACTED]® simplifies and reduces the risk of a hybrid cloud environment now and into the future through:

- Providing a consistent set of security controls across on-premises and multi-cloud environments requiring no network or application changes reducing complexity, improve operational efficiencies and lower IT security costs.
- Leveraging identity and cryptographic controls to quickly and easily segment any physical network into multiple logical microsegments
- Reducing the attack surface, encrypting data in motion, making endpoints invisible to unauthorized users and dramatically improving security and resiliency

As the Network and attack surface expands, risk increases. Ransomware and data breaches put citizens and employees at risk. We cannot prevent adversaries from trying to get in - But we can control an attack before it becomes a crisis. Unisys [REDACTED]® protects some of the world's most sensitive data across the public and private sectors.

[REDACTED]® is a software platform that easily allows any network to be logically segmented into smaller micro-segments and restricts communication to pre-authorized groups of users and devices called Communities of Interest (COI). [REDACTED]® COIs are cryptographically isolated from the underlying network infrastructure and each other.

[REDACTED]® reduces the attack surface, encrypts data in motion, makes endpoints invisible to unauthorized users, and dramatically improves security and resiliency. [REDACTED]® is “Identity Based” and integrates with existing identity services and processes [REDACTED] – enabling the least privilege and trusted communication.

[REDACTED]® replaces traditional network security technologies with software. Requiring no application changes or reconfiguration, [REDACTED]® can be easily integrated into the existing IT infrastructure with little or no disruption.

[REDACTED]® is highly scalable supporting on-premise, hybrid, and multi-cloud architectures. [REDACTED]® dramatically improves security, reduces complexity, is easy to manage, and lowers IT security costs.

- Works seamlessly with existing network architectures (on-premises, private cloud, and multi-cloud)
- Grants precise control over access and permissions
- Removes assumed trust from the equation allowing only safe connections
- Reduces audit scope by isolating systems with sensitive data

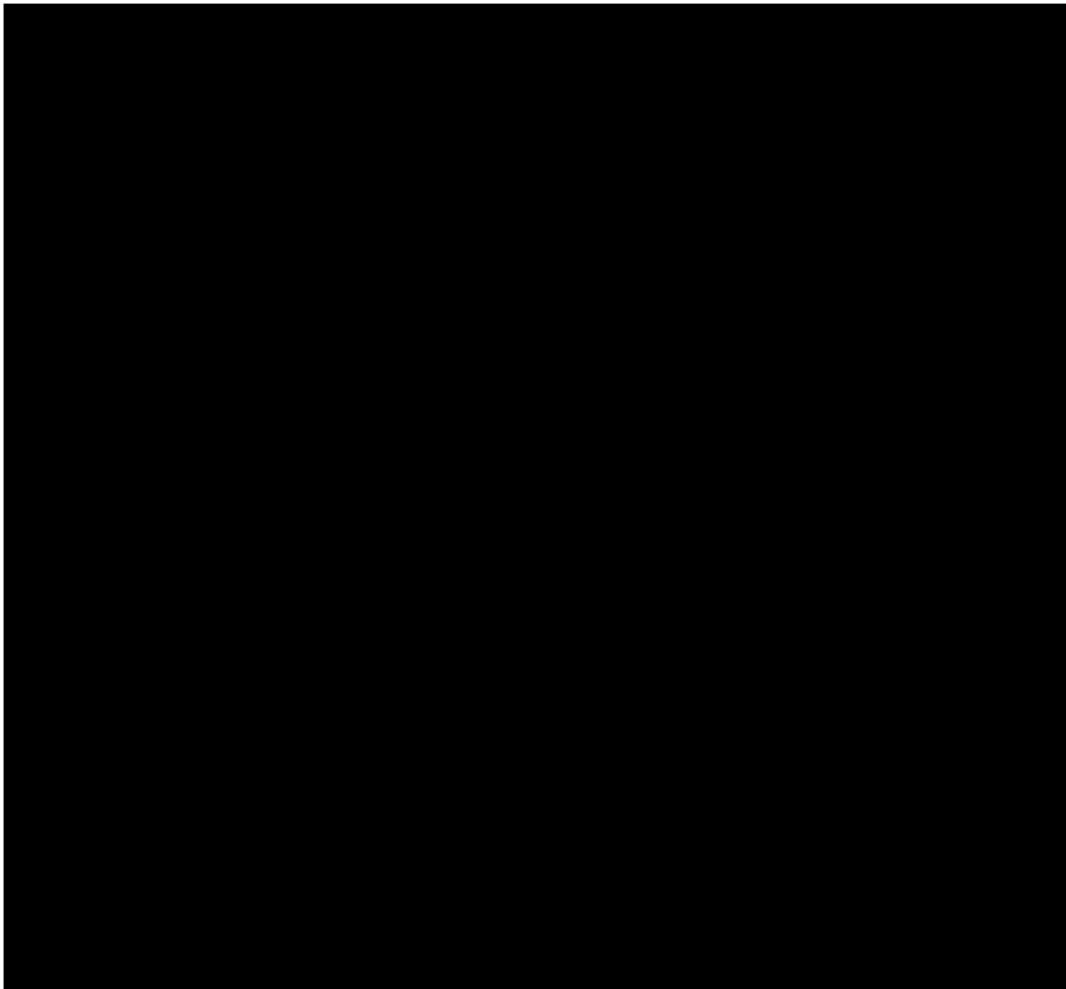
- Provides a layer of yet unbroken encryption that makes the rest of the network invisible, disrupting any unauthorized search for information or attempts to move laterally through the network

Each user, regardless of location or device, can only interact with the communities of people, devices, and data they need.

## ████████ ARCHITECTURE

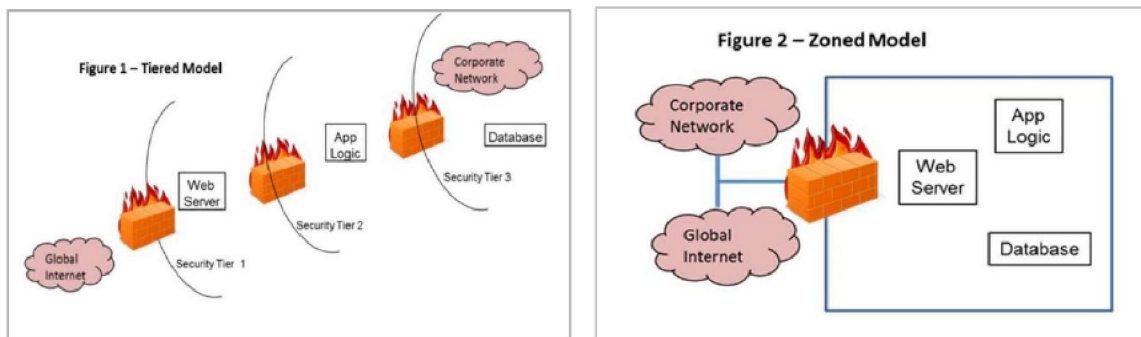
Unisys ██████████<sup>®</sup> is a highly scalable software-based, micro-segmentation platform that:

- Significantly reduces the operational cost of managing thousands of access control policies by creating flat, micro-segmented networks, eliminate the need for complex security policies and streamlines the change control process
- Secures sensitive data against internal and external threats by restricting lateral movement within across the extended enterprise
- Provides next-generation micro-segmentation security without the need to “rip and replace” underlying physical infrastructure, allowing a unified security posture that can be enforced from the primary data center to the disaster recovery site, public/private/hybrid cloud, offsite/branch office, and down to end-user laptops and mobile devices

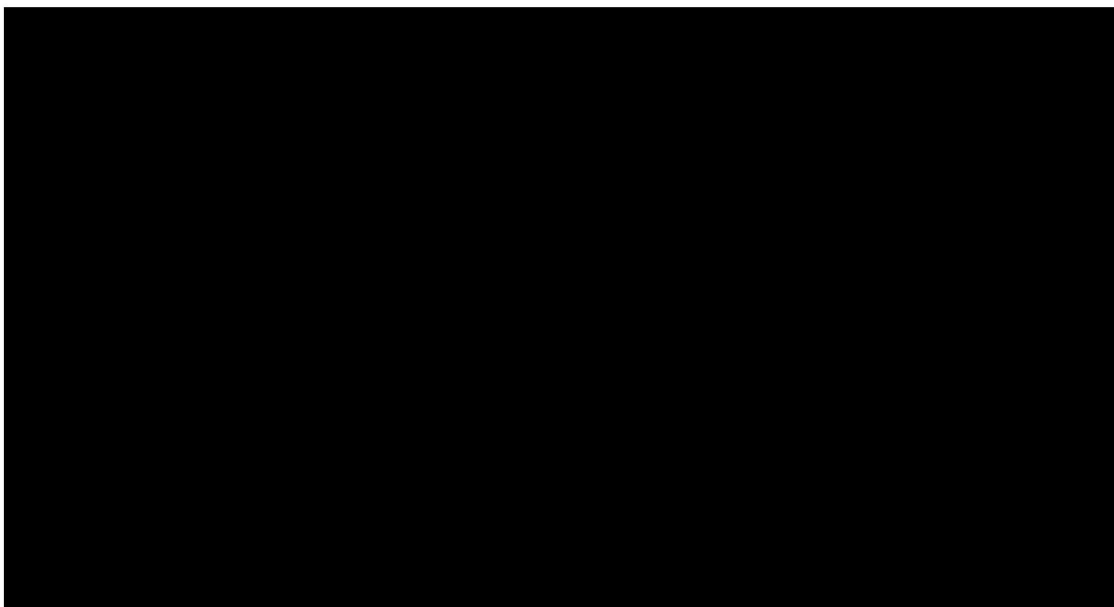




The traditional approach for segmentation relies on physical segmentation, which requires tiered or zoned architectures using VLANs and firewalls. This requires expensive and scarce resources to design, up-front capital expenditure on equipment, installation labor, and ongoing operations and maintenance expense – all contributing to the increasing cost of IT. Such traditional network segmentation approaches are also subject to increased risks arising from incorrectly configured VLANs and firewalls. For instance, if a configuration element is incorrect, VLANs “fail open” and a communication path is established. Maintaining multiple zones or tiers is expensive and complex, and managing user privileges that change as business requirements evolve can force physical network reconfigurations. For these reasons, many organizations fail to implement a secure, segmented environment.



In contrast, the figure below depicts how ██████████® overlays on a traditional “three-tier” security model and applies micro-segmentation.



██████████® uses ██████████ cryptographic algorithms and modules and adheres to a NIST-approved method for key exchange. This makes it suitable for protecting sensitive data-in-motion for mission-critical enterprises.

## FUNCTIONAL OVERVIEW

██████████<sup>®</sup> is a set of network security policy definition, distribution, and enforcement services. These services are distributed throughout the network and operate interactively to support a centralized management/distributed enforcement model. The sections below describe the functional aspects of ██████████<sup>®</sup> and outline the various ██████████<sup>®</sup> components and their functions.

██████████® is not a firewall, VPN, VLAN manager, or bulk encryptor, although there are aspects of all of these technologies built into ██████████®.

Rather, [REDACTED]® provides a “Zero-Trust” micro-segmentation capability based on the identity and/or role of users and servers within the organization. This Zero-Trust capability is built on a foundation of robust, military-grade cryptography that has been tested, endorsed, and given an Authority To Operate (ATO) on classified networks by the National Security Agency (NSA) and the U.S. Department of Defense (DoD).

Suite B level cryptography is used to enforce identity/role-based access to services in the network by users and other services. The primary method of enforcement is a concept known as Communities of Interest (COIs). In general, members of the same COI are allowed to communicate with each other within limits further imposed by IP address and service (Protocol+Port) level filtering.

Network nodes that are not members of the same COI are not visible to each other beyond ARPs on the local subnet. Attempts by nodes that are not [REDACTED] enabled to communicate with [REDACTED] enabled nodes are blocked silently, i.e., no response is returned, unless explicitly allowed by filtering policies. Through this means, [REDACTED]® endpoints are “dark” on the network – [REDACTED]

In the simplest terms, **██████████**® can be thought of as a policy management and enforcement solution which manipulates the OS-native communications stacks to enforce the user/role-based policies assigned to the **██████████**®-enabled endpoint.

## ████████ DEPLOYMENT

A typical deployment scenario for ██████████<sup>®</sup> involves several phases, including:

1. Using ██████████ to discovery what nodes are communicating and how they are doing so;
2. Using ██████████ to model role-based relationships between groups of nodes automatically;
3. Using ██████████ to model which nodes should be ██████████ enabled and the security policies to be applied to those nodes;
4. Mapping ██████████ modeled endpoint profiles to LDAP security groups;
5. Defining the modeled policies within the ██████████<sup>®</sup> management services;
6. Provisioning the role-based policies to authorization services distributed throughout the network;
7. Creating and distributing ██████████<sup>®</sup> endpoint agents to the ██████████ enabled nodes;
8. Endpoints being authorized into, and enforcing their respective ██████████<sup>®</sup> roles;
9. Logging and auditing management updates and endpoint operational events.

## ████████<sup>®</sup> COMPONENTS

████████<sup>®</sup> is implemented as a collection of services and virtual appliances (i.e., gateways) that are distributed throughout the enterprise. The services are organized into installable components which:

Discover and model the underlying network behaviors – ██████████;

1. Define and manage ██████████<sup>®</sup> policies and other components – Enterprise Manager (EM);
2. Authenticate, authorize, distribute policies, monitor, and control ██████████<sup>®</sup> endpoints – Standalone Authorization Servers (SAASes);
3. Enforce ██████████<sup>®</sup> policies, report on health and network activity, and support external Data Loss Prevention (DLP) and Deep Packet Inspection (DPI) technologies – Endpoint Agent.

██████████ devices can be integrated into ██████████<sup>®</sup> enclaves by using ██████████<sup>®</sup> gateways. These gateways front-end legacy and embedded devices on which a ██████████<sup>®</sup> endpoint agent cannot be installed. These “clear-text” devices can be represented by virtual ██████████ endpoints within the gateway and thereby participate fully in the ██████████ enterprise.

## ████████<sup>®</sup> GATEWAYS

The final set of components in the ██████████<sup>®</sup> product suite are gateways that allow devices that cannot be ██████████ enabled to participate in ██████████ protected networks. ██████████<sup>®</sup> gateways are software appliances that can be deployed as virtual machines or on bare metal.



██████<sup>®</sup> Secure Virtual Gateways (SVGs) are high-performance appliances that front-end legacy and other systems for which there is not a ██████<sup>®</sup> endpoint agent available. SVGs can be configured to apply different roles to individual or ranges of IP addresses. In this way, many non-██████<sup>®</sup> devices can be protected and segmented by SVGs, which can be scaled as performance demands.

#### ██████<sup>®</sup> PACKET INSPECTION ENABLEMENT

It is often mandatory that ingress and egress traffic (i.e., North/South traffic) be inspected to look for malicious activity and data exfiltration. Similarly, if a device in the network is suspected of having been compromised, security personnel may need to monitor and inspect that node's network traffic. If the traffic in question is ██████ enabled (i.e., encrypted and transmitted within an IPsec security association) inspection beyond the IP header is impossible.

The ██████<sup>®</sup> Packet Inspection Enablement (PIE) feature addresses this requirement. This feature does not itself inspect the traffic. Rather, it enables third-party inspection tooling by mirroring sent, received, and blocked clear-text and ██████ enabled traffic to a ██████<sup>®</sup> PIE Server where it is decrypted and reflected as clear-text traffic over a private network connection to the inspection tool, e.g., an Intrusion Detection.

### 12.1.5 Web Application Firewall

The Unisys Web Application Firewall (WAF) Cloud service is multi-tenant solution consisting of a web application security firewall, providing protection against sophisticated security threats. Cloud WAF is an integrated, defense in depth suite of application security and delivery services within the subscription providing ████████████████████. All components share intelligence so that security and delivery logic can be applied right from the edge, as soon as the request hits the WAF. The solution will be integrated with ██████████, and SaaS attack analytics uses artificial intelligence (AI) to distill thousands of Cloud WAF events into distinct narratives. Agencies will be able to have read only to view information about their sites.

Unisys WAF ████████████████████ protects against Open Web Application Security Project (OWASP) Top 10 security threats like cross-site scripting, illegal resource access, and remote file inclusion, blocking attacks in real time. Unisys WAF is configurable through ████████████████████. A simple GUI ████████████████████. A high-level Cloud WAF dashboard provides ████████████████████.

The Unisys WAF service consists of a classification engine that analyses all incoming traffic to customer's web sites with the aim of preventing malicious and unwanted traffic from entering the site.

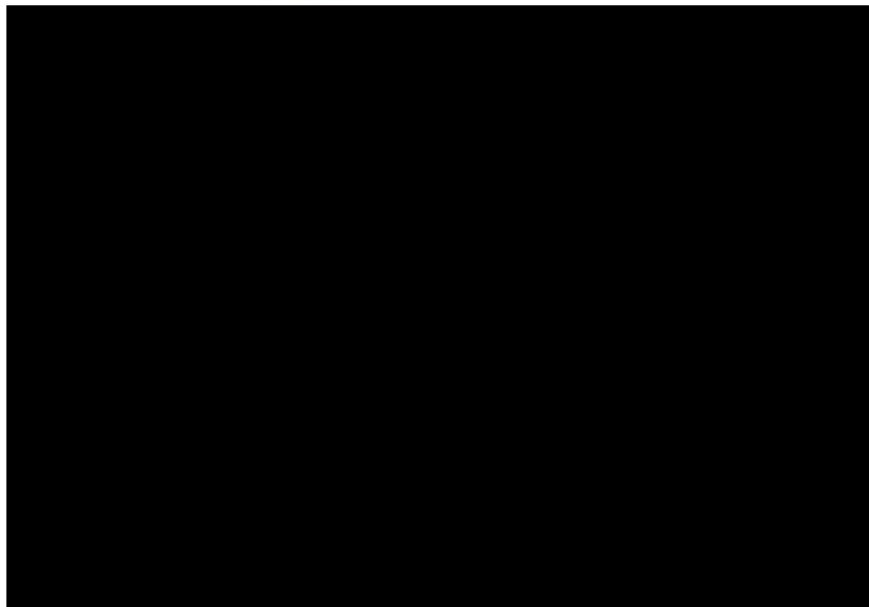


Unisys Cloud Web Protection is a 100% cloud-based solution for protecting websites and applications from external threats including: OWASP top 10 threats, automated attacks, hacking attempts, malicious bots, scraping and DDoS attacks.



### OWASP Top 10 and Automated Top 20

At the core of the Web Protection is the reverse proxy and Web Application Firewall (WAF), which are deployed across the cloud service distributed content delivery network. Website traffic is routed through the Cloud WAF [REDACTED]. This enables Cloud WAF to inspect website traffic requests and filter out any kind of malicious activity.



Pictorial View of the Unisys Cloud WAF Services

#### Cloud WAF Service Availability of 99.999%:

[REDACTED] provides what is called an advanced (smart mesh) Anycast network consisting of global Points of Presence (PoPs) that provide anywhere from [REDACTED] connections. VITA will only be using Continental U.S. PoPs and data centers. The applicable SLA for the WAF Services is set forth in Exhibit 3.1 and Exhibit 3.2.

#### Isolating Failover to NA:

The Cloud WAF provides the ability to isolate both data and failover/redundancy capabilities as



detailed above within a specific geographic region or even specific PoPs. The Cloud WAF Advanced Anycast network uses [REDACTED] to advertise routes that are made available when a failover requirement is met, and as such will be customized to our customers' requirements for data and/or failover/redundancy isolation. VITA will only be using Continental U.S. PoPs and data centers.

## WAF Features

The WAF features provided by these Services consists of the following for the Cloud and virtual appliance:

### Application Security

**Cloud Web Application Firewall** - A cloud WAF that protects applications against attacks wherever they're located; on-premises, in public or private cloud. [REDACTED] cloud WAF is PCI-certified, customizable, SIEM-ready and tuned for blocking threats with minimal false-positives..

**API Security** - Protects websites and APIs with an intuitive single stack approach. Enforces positive security models automatically, integrating seamlessly with leading API Gateway vendors.

**SIEM Integration** - Integration with leading Security Information and Event Management (SIEM) systems, including [REDACTED].

**Web Application Firewall Gateway** - An Agency appliance or virtual WAF that protects applications against attacks wherever they're located; on-premises, in public or private cloud.

### ANALYTICS

**Reputation Intelligence** - A security reputation feed combines research from security researchers, live crowdsourced intelligence from millions of sites and threat intelligence from multiple partners.

**Attack Analytics** - Uses machine learning to distill thousands of events into a single, actionable attack narrative. Provides a single consolidated event feed from both cloud and on-premises application security.

### APPLICATION DELIVERY

**Content Delivery Network** - Uses intelligent caching and cache control options, as well as high-speed storage and optimization tools to improve website performance while lowering bandwidth costs.

**Dynamic Content Acceleration** - Network acceleration boosts response times and leverages flexible routing to provide an optimized end user experience.

**Cache Shield** - Cache Shield provides the content delivery network with an intermediate cache layer to optimize infrastructure capacity. The service protects origin servers from redundant requests, sending

all requests to an automatically-selected point of presence (PoP).

**Load Balancing** - A cloud-based load balancer that supports local and global server load balancing across on-premises and public cloud data centers. Supports automatic failover to standby servers to enable high-availability and disaster recovery without any TTL-related delays.

## **BOT PROTECTION**

**Client Classification** - A multilayered system to block malicious traffic. Behavioral analysis, device fingerprinting, signature identification and transparent challenges combine to only allow legitimate users with low false positives.

**CAPTCHA Insertion** - Inserts CAPTCHA test into the workflow to mitigate automated bot traffic.

## **Data Security**

### **DISCOVERY AND ASSESSMENT**

**Data Discovery and Classification** - Discovers unknown databases by scanning the cloud network for database services and servers. Identifies sensitive data such as credit card numbers or national identification numbers.

**Database Vulnerability Assessments** - Scans databases for vulnerabilities and misconfigurations such as default passwords. Provides detailed reports including recommended remediation steps.

## **Data Protection**

**Data Activity Monitoring** - Continuously monitors database transactions, such as local privileged user and service account activity. Provides enterprise wide visibility of database activity across supported on-premises and cloud environments. Alerts or blocks based on security or compliance policy violations. Demonstrate compliance with predefined and custom reports.

**Data Security Gateways** - A virtual appliance that continuously monitors database activity. The Cloud WAF data security gateways provides for scalability, reliability and performance. Data security gateways can be deployed on-premises and in public or private clouds.

**User Rights Management** - Aggregates, correlates and reports on user access rights across heterogeneous enterprise databases.

## **Analytics**

**Data Risk Analytics** - Identifies dangerous data access activity that exposes sensitive data to breach risk. Uses machine learning, data science and behavior analytics to analyze and distill millions of database

events into a few actionable incidents.

## Cloud Data Security

**Cloud Data Security** - Allows quick on-boarding within minutes to obtain instant visibility of Agency cloud data, with automated discovery, classification, continuous monitoring, and security insights.

### Complimentary Distributed Denial of Service Attacks

Complimentary [REDACTED] DDoS protection is provided; however, if there are repetitive attacks, VITA will automatically be charged for the premium service resource unit as described in Exhibit 4.2 in the amount shown in Exhibit 4.1.

### Distributed Denial of Service Attacks Premium

DDoS Protection for Websites - An always-on DDoS mitigation service that manages any type, size or duration of attack with near-zero latency within seconds. Protects applications on-premises or in the cloud with activation via a simple DNS change.

## 12.2 Analytics Platform Service

Producing actionable insight and enabling evidence-based decision-making are paramount benefits, which can be accessed from underlying enterprise information systems. Elements in an IT enterprise as diverse as that of CoV will likely be at different maturation levels in their ability to benefit from the expansive and granular data sets now available. Unisys Advanced Analytics provides capability and solutions that span the full breadth of the data journey beginning with large-scale data collection, master data management, infrastructure solution, and progressing to full organizational transformation with integration of machine learning and predictive modeling (**Figures 12.2-1 and 12.2-2**). The desired path is not always linear; Unisys Advanced Analytics offers analytics as-a-service that supplements and enhances enterprise capability at a desired point in the data journey continuum. Advanced offerings include artificial intelligence applications, Machine Learning as-a Service, advanced systems modeling, and data scientists on demand to deliver services and consulting. Unisys has a library of off-the-shelf predictive models for finance, security, and transportation.



VITA has many opportunities to enhance the breadth and vibrancy of data analytics

Unisys Analytics Roadmap to Achieve Value

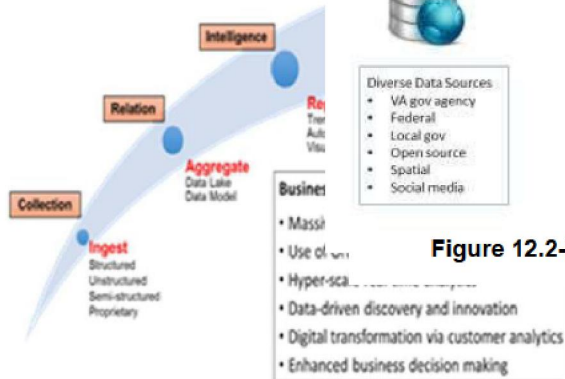


Figure 12.2-1. Data-Driven Transformation.

### VITA Advanced Analytics CoE Process Flow

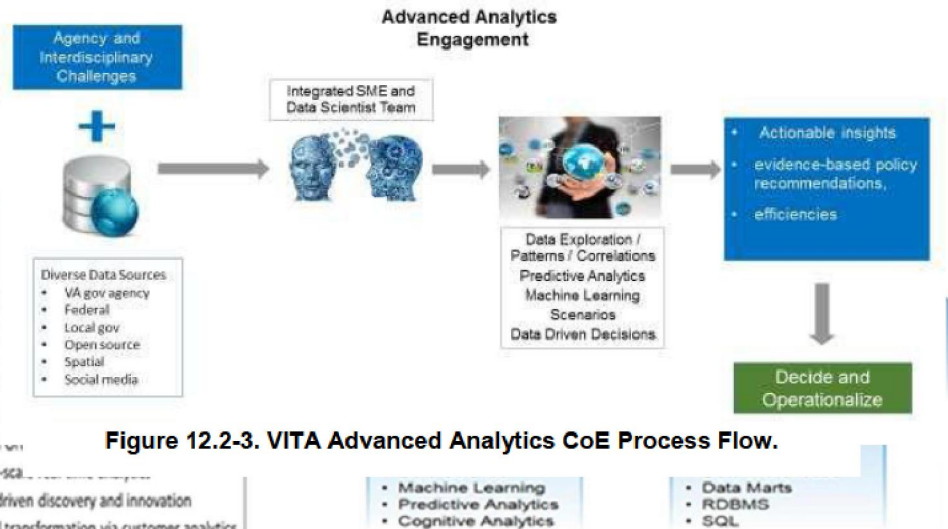


Figure 12.2-3. VITA Advanced Analytics CoE Process Flow.

Figure 12.2-2. Unisys Enterprise Data Management.

across the CoV enterprise, Customer by Customer, and for difficult interdisciplinary problem domains such as social welfare, security, health, equitable servicing, and environment.

Built into the cloud, U-APS is scalable on demand, permits flexible configurations, supports modular builds and decommissions, and supports multitenancy in which a library of developed structures is available to support future projects as the analytics system grows to encompass more of the enterprise. In the U-APS environment, a data lake integrates and stores data of interest: structured, semi structured, unstructured, and spatial. The data is then extracted for transformation and load to one or more of the data structures in the U-APS, or applications external to the U-APS, used to support reporting, analytics, and machine-learning applications to produce targeted insights. Depending on the data size and system requirements, typical U-APS design uses distributed databases, such as Cloudera Hadoop or Amazon's EMR to enhance U-APS performance across large volumes of data. The nonproprietary architecture of the U-APS supports a complete assemblage of scientific analysis and data visualization applications to integrate with the U-APS to include R, Python, SAS, ESRI ArcGIS, Amazon AI and ML, Tableau, ZoomData, and PowerBI.

The CoE is the hub of investigation for challenging problems requiring advanced analytics techniques for targeted solutions and generation of critical information to drive business and policy decisions as described in Figure 12.2-3.

In the CoE, problem statements are formed, domain knowledge and supporting data are gathered, approaches are developed, and cost-benefit analysis is produced. The CoE supports a continual cycle of request, study, and operationalization. Establishing a CoE clearly communicates a commitment to knowledge generation and evidence-based policy. The CoE serves as a hub for government, academic, and public coordination through sharing of data, techniques, and the knowledge produced therewith. Although there is ample work for a CoE with an inward focus, the CoE also has great potential as an integrator of government expertise and data with scientific/academic fervor and technique. Additionally, public and stakeholder participation in data-based

discovery can crowd source knowledge and foster support for policy initiatives backed by data-driven evidence.

## 12.3 Electronic Records Management Service

The explosion of unstructured content is one of the biggest challenges facing governments and businesses today. Because of regulatory and internal requirements, the tracking of customer and partner interactions, and the widespread use of office productivity suites, the quantities of documents, images, email, web content, audio, and video are growing at an astounding rate.

Based on the requirements in the SOW, Unisys recommends implementing our Infolmage solution, which is an Enterprise Content Management (ECM) platform with integrated Business Process Management (BPM/workflow) and Records Management (RM) for business-critical applications that involve high document volumes arriving as paper, electronic files, digital assets, email and internet transactions. Infolmage can easily capture, manage, store, and access the content required for cases, inquiries, and process-centric work, regardless of data structure or document origination, at a single intuitive user interface. Unisys Infolmage brings ECM, imaging, workflow, document management, Web and integration technologies together to form an integrated end-to-end solution. Unisys provides the core software and implementation expertise and services to deliver world class ECM solutions.

As the enterprise moves away from a fixed and location-centric work setting to a dispersed mobile world, the ability to interconnect people, processes, and core content becomes a necessity. Therefore, a mobile client for a contemporary enterprise content management suite is very essential. Infolmage also supports a well-featured mobile client on the Apple iPad and other mobile devices, allowing document retrieval by query search or retrieval and access from workflow queues as well as capturing images and creating new content items.

Infolmage is integrated with Microsoft SharePoint to serve as a content repository and a user interface. This capability combines Infolmage transaction processing solutions with a SharePoint environment's collaboration, content, and portal functionality. SharePoint is an integrated suite of capabilities that can help users to improve effectiveness by providing enterprise search, content management, and facilitated information sharing across the enterprise. Each Infolmage domain has a corresponding SharePoint document center, and each Infolmage document class has a corresponding SharePoint document library.

The open archive architecture of Infolmage Storage Manager allows the file system to function as a disk archive or to interface with content addressable storage or a Hierarchical Storage Management subsystem. This allows slower, low-cost storage to be used for less frequently accessed documents.

Infolmage offers an easy point-and-click approach to creating powerful and flexible content-centric workflows without writing code. Workflow rules are based on the metadata defined for incoming content, allow routing decisions to be made on process-specific values. Infolmage Workflow Designer allows VITA to easily automate its processes and integrate them with existing line-of-business applications.

Unisys implemented and supports hundreds of clients around the globe, in a wide variety of application areas. Solutions and implementations range from simple to very complex, and client end-user populations range from hundreds to many thousands in our large complex enterprise solutions. Client references and case studies are available from a diverse cross-section of many of the world's largest financial services and government organizations.

## 12.4 Intentionally Left Blank

## 12.5 Additional Database Services

Unisys' Managed Database as a Service (DBaaS) will provide additional Database Administration Services, including assistance with Database Design and Development Services. Our DBaaS will manage MS SQL Server, Oracle, and Oracle RAC Database platforms as well as AWS database formats by managing logical and physical databases. Unisys will provision "n" and "n-1" databases with infrastructure to take advantage of the self-provisioning and elasticity features of DBaaS capabilities. Unisys understands that the CoV continues to own Microsoft SQL Server licenses that are shared among VITA customers. For Oracle, VITA customers continue to own the licenses.

Following are more details on how certain aspects of Database services can be provided.

### Database segregation

In addition to access control, database segregation is accomplished by using two basic approaches.

1. Use of separate databases. Unless a connection is established between two databases even if they are installed on the same hardware and on the same database instance users of one database cannot access data on the second database. This separation is included in most modern database management systems including DB2, Oracle, Microsoft SQL and MySQL.
2. Network segregation. Different databases are configured on different virtual networks. The database can be configured to only accept connections from defined IP addresses and or subnets.

### Database migration

CGI basic approach to database migration is to make a full copy of the database, move that copy to the target infrastructure. For smaller database, the copy can be restored to the new infrastructure across network links. Moving larger database to a new datacenter may require the use of temporary media such as tape or disk and then physically transporting the media to the new target location. Once restored to the new target system incremental changes can be replicated over the network. Both Azure and AWS have services that utilize USB disks to recover large data sets to their respectively cloud storage systems.

Data virtualization may also be used for database migration. Data virtualization packages data in to lightweight pods and decouples the data from existing infrastructure. Because it's a full copy of the database (with data masking) it is possible to perform multiple practice cutovers before the final migration. Once actual cutover is scheduled the full data set can be restored.

### Database License Transferability

There are multiple licensing models to consider

### Infrastructure as a Service / Bring your own license

VITA may elect to transfer existing licenses for use on Unisys managed infrastructure. As the size of the DBaaS farm grows to exceed licenses transferred VITA can purchase additional licensing. Transfer of existing licenses is subject to the original purchasing terms. Depending on the terms of which existing licenses purchased this approach can be used for perpetual Oracle and/or SQL licenses. This approach preserves the



Commonwealth's investment in existing licenses. New license purchase agreements should include stipulations for transfer.

### **Infrastructure as a Service**

CGI/Unisys provides the licensing for Oracle and Microsoft databases. In the unlikely event of services termination, the Oracle licenses can be transferred to the Commonwealth. CGI/Unisys provided licenses for Microsoft SQL may not be transferred at termination. Microsoft obliges service providers such as CGI and Unisys to purchase licensing on a monthly subscription basis. There is no initial one-time charge for Microsoft Server Provider licenses (SPLA). And, because the software is purchased on a monthly subscription basis, there are also no licenses to transfer in the event of termination of services.

### **DBaaS**

For DBaaS Unisys would license the database instance by the number of cores. Termination charges (for remaining HW/SW (Oracle) amortization) would apply. Upon termination Oracle, not Microsoft SPLA licenses may be transferred to the Commonwealth.

### **Physical Servers**

Physical servers and databases are priced on a custom basis to meet VITA's specific requirements. CGI recommends physical servers for Oracle RAC clusters. Upon termination Oracle, not Microsoft SPLA licenses may be transferred to the Commonwealth.

## **12.5.1 Base Database Support**

Unisys and our partner CGI will support VITA's basic database support needs through a DBaaS model that leverages a shared DBA team. This team has experience with delivering DBA services to hundreds of clients including FedRAMP, PCI, and NIST compliant environments. Our teams have reviewed the VITA rules and have the ability to comply with all VITA compliance requirements. Our DBA team possesses the skills required to be successful in MS SQL, Oracle, and MySQL server deployments. This includes high availability pairs, RAC, and standalone services. Protecting that data is paramount to success. Through backups, synchronization, and disaster recovery support, VITA and its customers will know that the data in the databases are protected to industry-standard levels or higher. By using a shared team, Unisys and CGI can provide a cost-effective solution that supports VITA by a charge per database instance model. This allows VITA to scale at its desired rate and know that CGI will have the team supporting it to scale alongside with no disruption in service.

## **12.5.2 Extended Database Support**

VITA's extended database support will be delivered through CGI's infrastructure consulting practice. CGI will use skilled Database Engineering resources as needed by the hour to craft solutions to meet VITA and its customers' needs. This includes schema changes, database creation, and database changes. Additional capabilities available to VITA include performance testing and operating system and database performance tuning. The same skilled professionals who support CGI's many environments will be leveraged to provide VITA with the expertise for these database functions.

Unisys and CGI will provide additional Database Administration Services, including assistance with Database Design and Development Services, as needed by the hour, to craft solutions to meet VITA and its customers'

needs. This includes schema changes, database creation, and database changes. Additional capabilities available to VITA include performance testing as well as operating system and database performance tuning.

## 12.6 High Availability Services via Multi-site Solution

CGI's High Availability Services (HA) approach is to create cost efficient solutions that provide failover based on system criticality and required performance characteristics of each of VITA's critical systems. HA can be provided by using a single VM with failover in a protected VM cluster to elaborate geographically dispersed WAN separated systems that use special tools for load balancing, database synchronization and application cutover. High availability systems can be hosted in VITA Primary (QTS) and Secondary locations, the Cloud and/or at other vendor data centers. There are four primary approaches to HA.

1. Local redundancy, including database/application clustering, VM clustering, redundant components
2. Regional Mirroring, including database/application clustering, synchronous replication, low latency network, up to 62 miles of separation, load balanced
3. Global Mirroring, including database/application clustering, asynchronous replication, greater than 62 miles of separation, load balanced
4. Disaster Recovery, asynchronous data replication with Hot, Cool or Warm standby systems.

The terms Disaster Recovery (DR) and HA have often been used interchangeably. While HA can be part of a DR strategy, Unisys generally think of HA solutions as local fault tolerant solutions within the same geographic region. Because disasters can often affect entire regions, best practices for DR suggest that DR Failover systems are available (hot, warm, cold) in a geographically separate region. For "always on" type systems a solution may include load balanced systems using two datacenters within a region and a low cost disaster recovery in the cloud (Amazon, Azure). This type of solution maximizes throughput using the regional pairs and provides for several lower cost options for recovery in the event of a regional disaster.

- Cool – data is replicated to the Cloud, VMs are off (configured but not deployed) and activated when a disaster is declared. Only storage and a small per VM monthly fee are charged. This is the lowest cost cloud enabled DR.
- Warm – data is replicated to the Cloud, smaller than production VMs are turned on and/or a subset of VMs are turned on. When a disaster is declared VMs can be restarted at a size more consistent with production. Charges accrue for VMs and storage usage.
- Hot – data is replicated to the Cloud, production sized VMs are running and ready to receive work in the event of a declared disaster. The Hot site may act as a tertiary datacenter if necessary. Charges may be slight lower or about the same as a non-cloud datacenter

Variations of the Cool, Warm or Hot DR setups can be provided using CGI datacenters and/or colo datacenters such as Sungard. Generally, speaking recovering to cloud will be the lowest cost DR option.

Both Amazon Web Services (AWS) and Azure clouds permit the use of their private high-speed networks for replication between their respective regional and national datacenter locations. These network links do not use the public internet and have very low latency (relative to the distance between the datacenters). Also, these networks are charged on per GB transferred with no minimums, so VITA would only pay for the bandwidth they use.

CGI's HA solutions for VITA include documentation of the use and management of the proposed solution. Whether VITA's requirement is for local High Availability, Regional Mirroring, Global Mirroring or Warm/Cold DR

solutions, CGI's consultants will design a technology solution that can meet VITA's service level requirements for RTO/RPO. Additionally, CGI can work with VITA to understand and improve current HA/DR schemes and to help document the process, improve the manageability of the solution and to help minimize disruptions when the schemes are used.

## 12.7 VITA Customer Infrastructure Supporting Specific Application SLAs

In today's agile and customer-focused environment, Unisys understands that VITA and its customers need flexibility for additional SLAs focusing on individual application and business services. In addition to the standard infrastructure SLAs provided in *Exhibit 3.1 (Service Level Matrix)*, Unisys will work with VITA to define specific SLAs for applications. Unisys will be implementing the [REDACTED] toolset. Unisys will work with VITA to define specific application monitor templates and reporting parameters for requested applications. For additional APM, application optimization, or application code analysis, Unisys will work with VITA and the MSI to evaluate and recommend additional services based on APM platforms from [REDACTED].

## 12.8 Oracle Private Cloud Services

### Overview

VITA's new data center will be primarily [REDACTED] which is a strategic platform for virtualizing most servers. The [REDACTED] private cloud model helps to facilitate rapid and low-risk migration from the existing data center to the new co-location site; however, transitioning the existing agencies with Oracle Databases and Oracle Applications would require that the Commonwealth make significant investments in Oracle licensing to meet the required [REDACTED] licensing metrics and policy as associated with Oracle licensing policy and metrics.

The agencies most likely impacted by transitioning their current architecture to [REDACTED] private cloud:

- Virginia Department of Taxation
- Virginia Department of Transportation
- Virginia Department of Social Services
- Virginia Department of Motor Vehicles
- Virginia Department of Health
- Virginia Information Technologies Agency

A private cloud solution within the new data center to host these specific Commonwealth agencies with Oracle database and applications is one that will substantially eliminate the need for Commonwealth agencies to purchase additional Oracle database licensing to migrate their existing environments to the new data center.

The solution will host multiple Oracle databases and Oracle applications within close network proximity to the non-Oracle servers and applications to meet application performance requirements.

Additional requirements consist of:

- Supports Oracle databases and Oracle applications



- Mitigates migration risks by leveraging the same OS
- Provides DR services to agencies
- Meets the applicable SLAs.
- Incorporates VITA's Enterprise Services model.

Assumptions on which the private cloud solution is based are:

- The solution will be installed at the new co-location data center in [REDACTED] Virginia
- The solution will also be installed at the DR site to support DR requirements

**Solution Components**

The private cloud solution will deploy Oracle's Private Cloud solution in the [REDACTED] data center as well as the DR data center to host the specific agencies listed above. These specific environments have business requirements that preclude them from migrating their current enterprise environments to Oracle OCI at this point. The described solution would not impact the Cardinal OCI solution nor the other agency applications that can be deployed within Oracle OCI.

The primary use case is Oracle Linux VMs running Oracle licensed software (e.g. Oracle Database) but the dedicated resource model may provide other use cases for applications with constraints around reserved core and memory resources, such elements to be agreed upon by the parties.

Oracle Private Cloud will integrate with the new data center networks via 10/25/40 or 100 Gb Ethernet to deliver a wire-once private cloud solution in the applicable datacenter. The environment will be connected to the high-speed LAN spine network to provide low latency interactions with other application components and other agency applications located in the data center. The solution is based on leveraging the data center's existing TIER1 SAN.

This solution adds a second "landing zone" for Oracle databases and applications and provides a choice between the OCI cloud and the VITA Oracle private cloud.

**Solution Attributes**

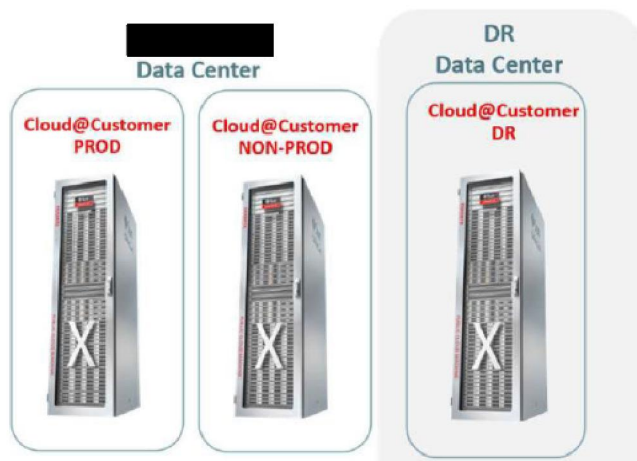
The solution:

- Supports Oracle DB and Oracle applications and current versions of Solaris (x86)
- Does not require the specified agencies to invest in additional Oracle database licensing to migrate their existing architectures to the PCC solution. The solution is based on each agency utilizing their existing, owned, on-premise based Oracle database licensing; no additional licensing is included in the solution.
- Provides for low latency connections to other applications and components.
  - Network Proximity with other Commonwealth workloads at the primary data center
- Delivers business continuity
  - Existing RUs for Disaster Recovery
  - SRDF data replication for TIER1 SAN
- Consists of an intelligent and agile infrastructure

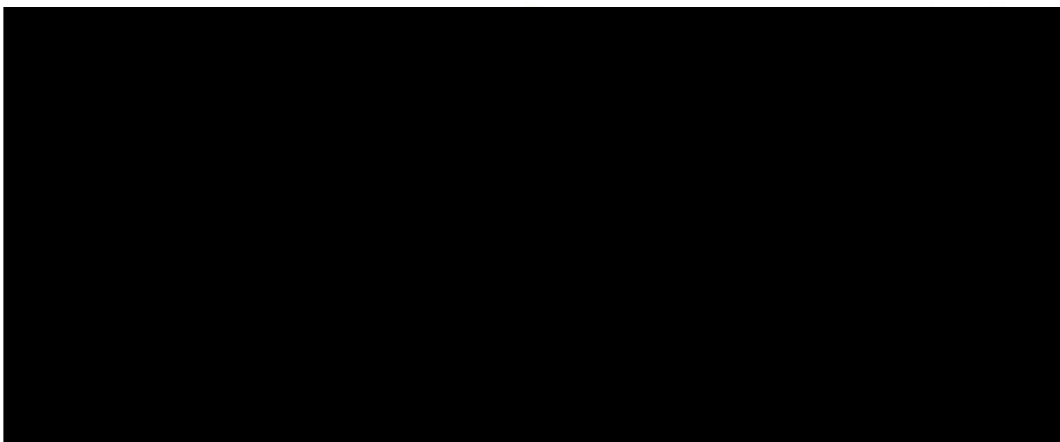
- Rapid scaling compute
- Software-defined networking
- Rapid scaling, TIER1 SAN
- Allows for Zero-downtime appliance upgrades
- Provides unified management with Oracle Enterprise Manager
  - Single pane management, monitoring
- Aides in security through Isolated Customer and Management Networks

### Proposed Configuration

The solution utilizes a two rack Oracle PCA deployment in the primary data center and a single rack deployment in the DR data center. The implementation can be scaled out in-rack in 48 core/1536 Gigabyte increments and by adding additional racks as the need to meet agency requirements.



Oracle Private Cloud: DR Architecture



### Agencies Targeted for the Private Cloud Solution

The Oracle Private Cloud Appliance (PCA) solution sizing is based solely on the agencies identified above and the Notes column in Table 1 below.

Table 1 Applicable Agencies and Assumptions

COVA Agency	Total Cores	Notes
VDH	124	
VDOT	700	
DSS	260	
TAX	412	
DMV	288	
VITA	40	
VSP	0	
Subtotal	1824	Assumptions Above

### Solaris

Commonwealth agencies with Solaris based architecture will require a time and materials discovery to confirm database and application migration to the proposed PCC solution through the RFS process and charged accordingly. Pricing for the Private Cloud Services consists of the core counts for Solaris systems as indicated below, but does not include converting any of the Solaris to Linux or Solaris x86.

- Virginia Department of Health – 17 servers, 124 cores included in this proposal
- Virginia Department of Motor Vehicles 9 servers, 84 cores included in this proposal
- Virginia State Police – Not included

Service Delivery Plan includes Application Planning & Modeling of the above-specified agencies (to be delivered under the custom RFS).

- Kick-off meeting
- Conduct a detailed analysis of all relevant SPARC/Solaris Systems and related applications. Including database and applications versions and dependencies, CPU, memory, storage, system capacity as applicable) and planning (e.g., migration approach);
- Analysis of the data
- Generate a report of findings and recommendations
- Collect and maintain configuration data that identifies all of the components (“Configuration Items”)
- Provide a detailed report of recommendations
- Conduct a final meeting to review the migration summary report.

### Deployment and Commitment Periods

Unisys will scale out both QTS and DR to provision the required infrastructure to meet the deployment and data center move (DCM) timeline. All installed capacity (cores and memory) become committed minimum from the date VITA or Customer certifies in writing that the installed capacity is ready for Customer use through the end of the commitment period (11/30/2024).

If additional scaling is required following the deployment period and VITA will negotiate the terms of such adjustments through the change order process of the Agreement.



## Resource Units

The Oracle Private Cloud Service will be charged under two new Resource Units and leverage existing Resource Units as referred to below.

- New Resource Units (See Exhibit 4.2 Resource Unit Definitions)
  - Oracle Private Cloud Dedicated Virtual Cores
  - Oracle Private Cloud Dedicated Virtual Memory
- Existing Resource Units (See Exhibit 4.2 Resource Unit Definitions)
  - Software Service Charge Linux OS
  - Software Service Charge Solaris
  - Server Support Services – Virtual (Primary DC), Linux Tier 2
  - Server Support Services – Virtual (Primary DC), Windows Server Tier 2
  - Server Support Services – Virtual (Primary DC), UNIX
  - Storage Service (Primary DC), Storage SAN Tier1
  - Disaster Recovery Services, Tier 1 (RTO , 4 hours)
  - Disaster Recovery Services, Tier 2 (RTO 4-24 hours)
  - Disaster Recovery Services, Tier 3 (RTO 25-48 hours)
  - Disaster Recovery Services, Tier 4 (RTO 49-72 hours)

Disaster Recovery is optional on a per server basis and incurs the existing Disaster Recovery Resource Unit cost per month and replicated storage cost in addition to the Oracle Private Cloud core and memory fees.

## 12.9 Secure Rack Hosting Services for Agency 3<sup>rd</sup> Party Equipment

### Overview

The Commonwealth standards require that all Commonwealth data processing and storage must reside in an approved “Tier 3” data center facility. Some Agencies utilize services from 3<sup>rd</sup> party suppliers that provide hardware and/or services to process Commonwealth data.

### Proposed Solution

To provide a solution for 3<sup>rd</sup> party equipment, Supplier will facilitate hosting of “secure racks” in Supplier’s hosting provider’s facility. The secure racks will be connected to the Commonwealth network [REDACTED]

**Existing Resource Units**

- Cross Connects

**New Resource Units**

- Secure Rack Hosting Service
- Redundant 30 AMP Power
- Redundant 50 AMP Power

**Labor**

- Smart Hands Labor

**Deployment and Commitment Periods**

Minimum commitment period for rack, power and cross connects is 12 months, renewable in 12 month increments. Unless written notice is provided by the Customer 120 days prior to the end of the current term, supplier will renew for 12 months. All Customer installed equipment and parts must be removed from the rack by the Customer prior to the end of the term. If notice of termination has been provided but the equipment has not been removed from the secure rack, monthly charges for rack and power will continue at 150% of the contract rate for any month or portion of a month that the rack continues to have Customer installed parts.